Cloud and Hybrid Deployments for Cisco Jabber 12.1

First Published: 2018-07-12

Last Modified: 2018-09-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

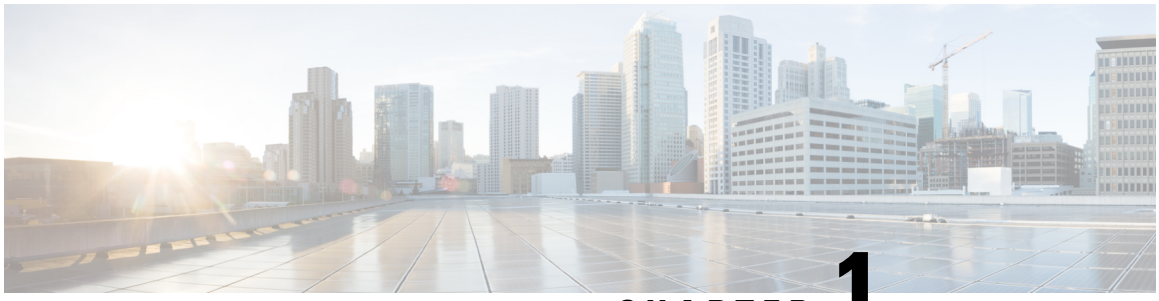
New and Changed Information

New and Changed Information

Description of Change	Status	Where Documented	When Documented
RESET_JABBER installation parameter	Added	Install Cisco Jabber for Windows	September 2018
Cisco Jabber Diagnostics Tool	Updated	*Troubleshooting* section	July 2018

New and Changed Information

CONTENTS



CHAPTER 1

Jabber Overview 12.1

Purpose of this Guide

This guide includes the following task-based information required to deploy and install Cisco Jabber:

- Configuration and installation workflows that outline the processes to configure and install cloud or hybrid deployments.
- How to configure the various services that the Cisco Jabber client interacts with, such as IM and Presence Service, Voice and Video Communication, Visual Voicemail, and Conferencing.
- How to configure directory integration, certificate validation, and service discovery.
- How to install the clients.

Before you deploy and install Cisco Jabber, see the *Cisco Jabber Planning Guide* at https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html to determine the deployment options that best suit your business needs.

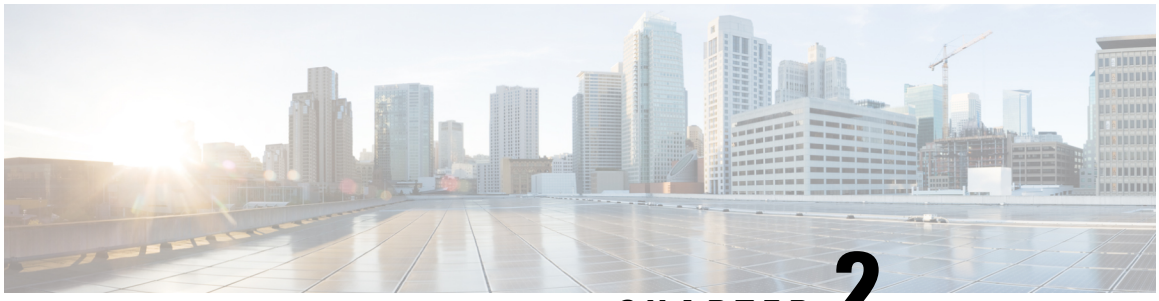
About Cisco Jabber

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing.

The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Android
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber Softphone for VDI

For more information about the Cisco Jabber suite of products, see https://www.cisco.com/go/jabber or https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html .



CHAPTER 2

Workflows for Cloud and Hybrid Deployments

Workflow for a Cloud Deployment using Cisco Webex Messenger

Procedure

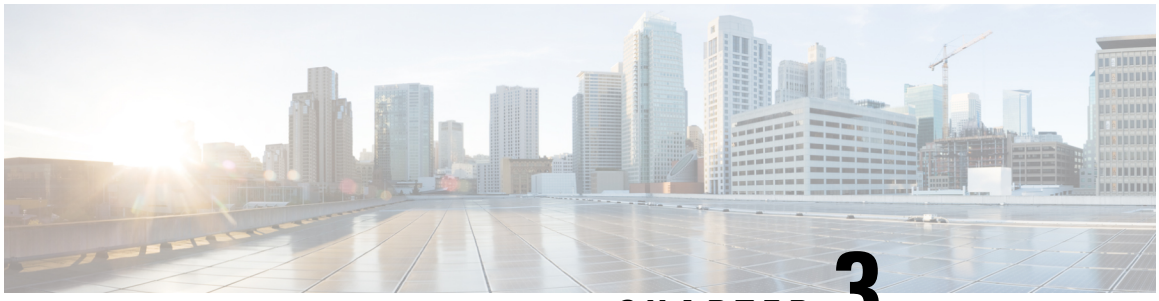
	Command or Action	Purpose
Step 1	Configure Policies, on page 5	
Step 2	Create Users for Cloud Deployment, on page 15	
Step 3	Set Up Certificate Validation, on page 51	
Step 4	Configure the Clients, on page 53	
Step 5	Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 63	

Workflow for a Hybrid Deployment using Webex Messenger

Procedure

	Command or Action	Purpose
Step 1	Configure Policies, on page 5	
Step 2	Configure Clusters, on page 11	
Step 3	Create Users for Hybrid Deployment, on page 23	
Step 4	Configure Softphone, on page 35	

	Command or Action	Purpose
Step 5	Configure Deskphone Control, on page 29	
Step 6	Configure Extend and Connect, on page 45	
Step 7	Configure Service Discovery for Remote Access, on page 49	
Step 8	Set Up Certificate Validation, on page 51	
Step 9	Configure the Clients, on page 53	
Step 10	Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 63	
Step 11	Remote Access, on page 101	



CHAPTER 3

Configure Policies

Add a Policy

Procedure

Step 1 Select the **Policy Editor** tab.
The **Policy List** appears to the left and the **Action List** appears at the right of the **Policy** screen.

Step 2 Under **Policy List**select **Add**.
The new policy appears at the top of the list of existing policies.

Step 3 Enter a unique name for the policy.

What to do next

To add actions for this policy, see Add Actions to a Policy, on page 5

Add Actions to a Policy

Procedure

Step 1 Select the **Policy Editor** tab.
The **Policy List** appears to the left and the **Action List** appears at the right of the **Policy Editor** screen.

Step 2 Under **Policy Name** select the policy to which you want to add actions.

Step 3 To add actions, select **Add** under **Action List** on the right of the screen.
The **Action Editor** screen appears.

Step 4 Select a policy action from the **Action Tag Name** list.

Step 5 Select **Save**.

Step 6 Repeat Steps 3-5 until all of your policies have actions assigned to them.

Policy Actions in Cisco Webex

By default, a newly provisioned Cisco Webex organization has all the capabilities granted to all the users.

Note The end-to-end encryption policy is not enabled by default. The Organization Administrator can enable this policy. Administrators can create policies when specific capabilities for all the users or specific groups of users need to be disabled.

Policy actions cannot be enforced on users using third-party XMPP IM applications.

No more than ten VoIP conference attendees can be connected to the same VoIP conference simultaneously.

External users are users who do not belong to the Cisco Webex organization. They can still use Cisco Webex to communicate with users who belong to the Cisco Webex organization.

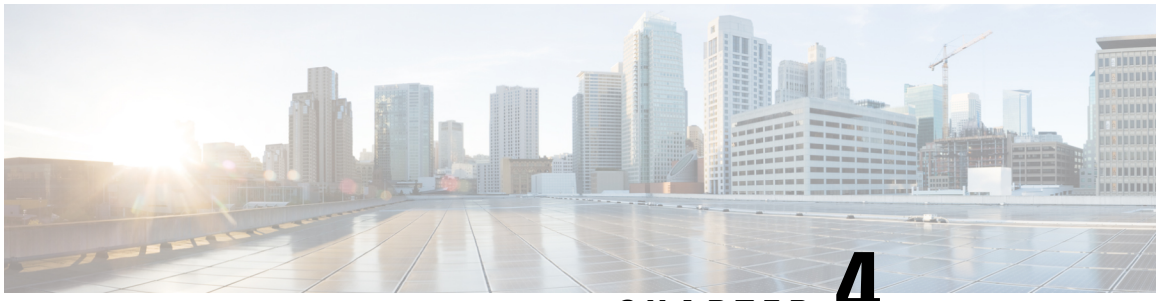
Policy Action	Description	Impact	Default Value
External File Transfer	Controls file transfer in an IM session between organization users and users outside the organization.	**Disabled**—Stops all file transfers between the organization users and external users. This includes multiparty IM sessions with at least one external user.	**Enabled**
Internal File Transfer	Controls file transfer in an IM session between users within the organization.	**Disabled**—Stops all internal file transfers. **Enabled**—All the users within the organization can exchange files with the internal users.	**Enabled**
External IM	Controls IM sessions between users in the organization and users outside the organization.	**Disabled**—Stops all IM sessions between users in the organization and users outside the organization. This stops all dependent services like voice, video, and VoIP.	**Enabled**

Policy Action	Description	Impact	Default Value
External VoIP	Controls VoIP communications in IM sessions between users in the organization and users outside the organization	**Disabled**—Stops all VoIP communications in IM sessions between users in the organization and users outside the organization. However, other services like text-based IM sessions and file transfers are available	**Enabled**
Internal VoIP	Controls VoIP communications in IM sessions between users within the organization.	**Disabled**—Stops all VoIP communications in IM sessions between users within the organization. However, other services like text-based IM sessions and file transfers are available. **Enabled**—All the users within the organization can use VoIP communications in IM sessions.	**Enabled**
External Video	Controls video services in IM sessions between users in the organization and users outside the organization	**Disabled**—Stops all video services in IM sessions between users within the organization and users outside the organization. However, other services like text-based IM sessions and file transfers are available.	**Enabled**
Internal Video	Controls video services in IM sessions between users within the organization.	**Disabled**—Stops all video services in IM sessions between users within the organization. However, other services like text-based IM sessions and file transfers are available. **Enabled**—All the users within the organization can use video communications in IM sessions.	**Enabled**

Policy Action	Description	Impact	Default Value
Local Archive	Controls the ability of the user to locally archive IM text messages.		**Enabled**
External Desktop Share	Controls the ability of users within the organization to share their desktop with users outside the organization.	**Disabled**—Prevents users within the organization from sharing their (local) desktop with users outside the organization. **Enabled**—Users can share their (local) desktop with users outside the organization.	**Enabled**
Internal Desktop share	Controls the ability of users within the organization to share their desktop with other users within the organization.	**Disabled**—Users within the organization can't share their desktop with other users within the organization. **Enabled**—Users can share their desktop with other users inside the organization.	**Enabled**
Support End-to-End Encryption For IM	Specify support for end-to-end Encryption for IM sessions.	**Enabled**—Support end-to-end Encryption for IM sessions. End-to-end encryption is not supported for logged users.	**Disabled**
Support NO Encoding For IM	Controls whether applications with end-to-end encryption enabled can start an IM session with applications that do not have end-to-end encryption enabled or with 3rd party applications that do not support end-to-end encryption.	**Disabled**—Prevents applications with end-to-end encryption enabled from initiating an IM session with applications or 3rd party applications that do not have end-to-end encryption enabled. **Enabled**—Encryption level negotiated is the highest level that the other party supports.	**Enabled**

Policy Action	Description	Impact	Default Value
Internal IM (including White Listed domains)	Controls IM communication between users within the organization and specific domains on the white list.	**Disabled**—Prevents users within the organization from being able to IM users within the domains specified in the white list. However, users within the domain can start an IM with each other. Also disables other dependent services such as VoIP, Video, and File Transfer.	**Enabled**
Upload Widgets			**Enabled**
Allow user to edit profile	Controls the ability to restrict users from editing their profile information.	**Disabled**—Prevents users from editing their profile information. This policy action impacts the settings in the **Profile Settings** screen under the **Configuration** tab.	**Enabled**
Allow user to edit the view profile setting	Controls the ability to restrict groups of users from changing their user profile view settings.	**Disabled**—Prevents users from changing their user profile view settings. This policy action impacts the **Allow users to change their profile view settings** check box in the **Profile Settings** screen under the **Configuration** tab. The **Allow users to change their profile view settings** check box has no impact even if it is selected.	**Enabled**
Internal Screen Capture	Controls users' ability to send a screen capture to users within the organization.	**Disabled**—Prevents users within the organization from sending screen captures within the organization.	**Enabled**
External Screen Capture	Controls users' ability to send a screen capture to users outside of the organization.	**Disabled**—Prevents users within the organization from sending screen captures outside of the organization.	**Enabled**

Policy Action	Description	Impact	Default Value
Send Internal Broadcast Message	Controls users' ability to send broadcast messages to users within the organization.	**Disabled**—Prevents users within the organization from sending broadcast messages inside the organization.	**Enabled**
Send External Broadcast Message	Controls users' ability to send broadcast messages to users outside of the organization.	**Disabled**—Prevents users within the organization from sending broadcast messages outside of the organization.	**Enabled**
Allow user to send broadcast to a directory group	Controls users' ability to send broadcast messages to a directory group within the organization.	**Disabled**—Prevents users within the organization from sending broadcast messages to a directory group within the organization.	**Enabled**
HD Video	Controls the HD Video feature on computer to computer calls when External Video or Internal Video policies are enabled	**Disabled**—Prevents HD Video for all computer to computer calls.	**Enabled**



CHAPTER 4

Configure Clusters

Configure Visual Voicemail

Procedure

Step 1 To configure Visual Voicemail, select the **Configuration tab** > **Unified Communications**.
The **Unified Communications** window opens.

Step 2 Select **Voicemail** to open the **Default settings for Visual Voicemail for CUCI** screen.

Unity Connection customers should enter the Unity Connection server IP Address or DNS name into the "Voicemail Server" and "Mailstore Server" fields. It is recommended that all other settings remain as the defaults.

Step 3 To enable Visual Voicemail, select **Enable Visual Voicemail**.

Step 4 If you want to manually enter the Visual Voicemail settings, select **Allow user to enter manual settings**.

Step 5 Enter the following information:

- **Voicemail Server**: Name of the Visual Voicemail server with which the Cisco Webex application should communicate for retrieving voicemail.
- **Voicemail Protocol**: Protocol used for communicating with the Visual Voicemail server. You can select HTTPS or HTTP.
- **Voicemail Port**: Port associated with the Visual Voicemail server.

The following Mailstore parameter options are not supported. The Cisco Webex Administration tool requires values, enter `10.0.0.0` as the Mailstore Server and use the default values for the remaining fields.

- **Mailstore Server**: Name of the mailstore server.
- **Mailstore Protocol**: Protocol used by the mailstore server. You can select TLS or Plain.
- **Mailstore Port:** Port associated with the mailstore server.

- **IMAP IDLE Expire Time**: Time (in minutes) after the expiry of which the server stops automatically checking for voicemail.
- **Mailstore Inbox Folder Name**: Name of the inbox folder configured at the mailstore server.
- **Mailstore Trash Folder Name**: Name of the trash folder (typically, the deleted items folder) configured at the mailstore server.

Step 6 Select **Save**.

Configure Cisco Unified Communications Manager Integration

Procedure

Step 1 Select the **Configuration tab** > **Additional Services > Unified Communications** .

Step 2 Select the **Clusters** tab and select **Add**.

Step 3 Select **Enable Cisco UC Manager integration with Messenger Service Client**.

Step 4 Select **Allow user to enter manual settings**, users can change the Primary Server values in basic mode or the TFTP/CTI/CCMCIP server values in advanced mode.

Note When this option is enabled, the user-entered settings will override the default or global Cisco Unified Communications Manager settings specified for the Cisco Webex organization.

Step 5 Under **Cisco Unified Communications Manager Server Settings**, select:

- **Basic Server Settings**: to enter the basic settings for the Cisco Unified Communications Manager server.
- **Advanced Server Settings**: to enter detailed settings for the Cisco Unified Communications Manager server.

  Note The server configuration options change based on: Basic or Advanced.

Step 6 Enter the following values for **Basic Server Settings**:

- **Primary Server**: Enter the IP address of the primary Cisco Unified Communications Manager server. This server is configured with TFTP, CTI, and CCMCIP settings.
- **Backup Server**: Enter the IP address of the backup Cisco Unified Communications Manager server. This server is configured with TFTP, CTI, and CCMCIP settings and provides failover support in case the primary Unified Communications Manager server fails.

Step 7 If you have selected **Advanced Server Settings**, specify each setting for TFTP (Trivial File Transfer Protocol), CTI (Computer Telephony Integration), and CCMCIP (Cisco Unified Communications Manager IP Phone) servers.

Step 8 Enter the IP address for each of the following servers:

Note You can specify up to two backup servers for the TFTP server and one backup server each for the CTI and CCMCIP servers. Enter the appropriate IP addresses for each Backup Server.

- **TFTP Server**
- **CTI Server**
- **CCMCIP Server**—This is the address of Cisco Unified Communications Manager (UDS) server.

The servers listed must be in the home cluster of the users.

Step 9 In the **Voicemail Pilot Number** box, enter the number of the voice message service in your Cisco Unified Communications server.

The Organization Administrator typically provides a default voice message number for your entire Cisco Webex organization. However, you can select the **Allow user to enter manual settings** check box to enable users of the cluster to override this default voice message number.

Step 10 Select **Voicemail**.

Step 11 Select **Enable Visual Voicemail**.

The Visual Voicemail settings entered here are applicable only to the users belonging to this cluster.

Step 12 In the **Clusters** tab, select **Specific voicemail server for this cluster** to specify a voicemail server, which is different from the voicemail server settings provided for the entire organization.

Step 13 Select **Allow user to enter manual settings** to permit users to manually enter Visual Voicemail settings for this cluster.

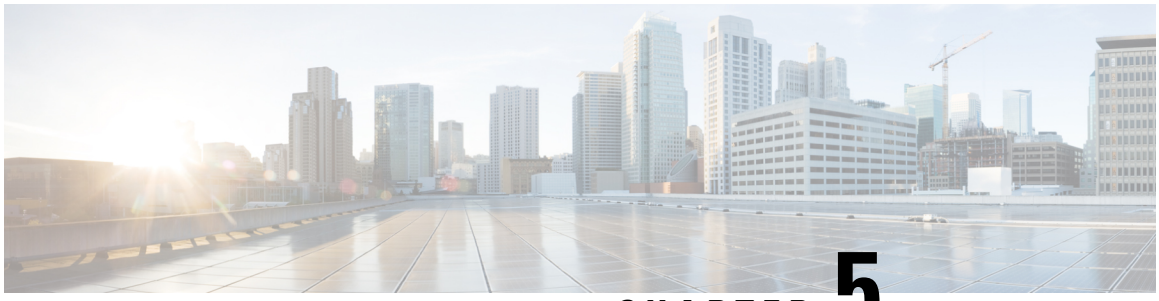
Step 14 Enter the following information:

Voicemail Server	Enter the IP address or FQDN for the Voicemail server
Voicemail Protocol	Select either HTTP or HTTPS
Voicemail Port	Enter the Port number

The Mailstore Server information is not supported, the Cisco Webex Administration tool expects a value for this field, enter `10.0.0.0`. The mailstore Protocol, Port, and IMAP IDLE Expire Time fields are not supported, do not delete the default values from these fields.

Mailstore Inbox Folder Name	Name of the inbox folder configured at the mailstore server
Mailstore Trash Folder Name	Name of the trash or deleted items folder configured at the mailstore server

Step 15 Select **Save** .



CHAPTER 5

Create Users for Cloud Deployment

Create Users Workflow

Cisco Webex Administration Tool provides a number of ways to create users for your organization.

Procedure

	Command or Action	Purpose
Step 1	Create users in Cisco Webex Administration Tool using one of the following methods: • You can add users individually using the Cisco WebexAdministration Tool. Create New Users, on page 16 • You can generate an email invitation for users to self register for a Cisco Webex account. User Provisioning Information, on page 16 • Create and import a CSV file with your users information. Create and Import a CSV File, on page 18	
Step 2	Assign users to policy groups. Assign Users to Policies, on page 21	

Create New Users

Procedure

Step 1 To create a new user or administrator, select the **User tab** > **Add**.

Step 2 Enter information in each field. The default Role is User (non-administrator).

Note The Business Email is the Username. You cannot edit the Username.

Step 3 (Optional) Select the **Policy Group Assignment** tab to assign a policy group to the user.

Step 4 If IM Archiving is enabled for your Cisco Webex Messenger Organization, the **Archive IMs** check box is displayed on the **Add User** dialog box. To log IMs for this user for archival, select the **Archive IMs** check box.

Step 5 To change the endpoint, select a different endpoint from the drop down list.
Selecting **Default** assigns the user to the endpoint preconfigured as the default endpoint in the **IM Archiving** screen.

Step 6 To assign this user to an upgrade site, select a site from the **Upgrade Site** drop-down list.

Step 7 If your Cisco Webex Messenger Organization is enabled with Cisco Unified Communications, the Unified Communications tab is displayed on the Add User dialog box. Select the **Unified Communications** tab to view the settings available for Cisco Unified Communications.

Step 8 Under **Cluster**, select the applicable Cisco Unified Communications cluster to which you want to add this user.

Step 9 If your Cisco Webex Messenger Organization is enabled with Cisco Webex Meeting Center integration, the Add User dialog box is displayed. To assign the Organization Administrator role to the user, select the **Organization Administrator** check box.

Note
- If you have enabled **Automatically enable Meeting account when creating a new user** in the **Meetings** page, the **Meeting Account** check box is selected by default. In such a case, you cannot clear the Meeting Account check box.
- When the **Meeting Account** check box is selected, it means a corresponding Cisco Webex Meeting Center account is created for this user.

Step 10 Select **Save.**

New users receive a welcome email based on the Welcome Email template in Cisco WebexMessenger Administration Tool.

Step 11 Repeat the previous steps to continue adding new users.

User Provisioning Information

User provisioning includes specifying user-provisioning information such as registration, and fields required when creating a user's profile. The settings you make here impact when users are provisioned in your Cisco

Webex Messenger Organization. For example, if you set specific fields as mandatory here, the user needs to compulsorily fill in those fields when creating the user profile.

Cisco Webex Messenger customers can enable self-registration when there is no SAML or Directory Integration enabled. In such a case, the Organization Administrator does not need to specify the registration URL. When registration is not enabled, customers can specify a custom web page. Any user trying to register with an email address that matches with customer's domain is redirected to the custom web page. Customers can use this webpage to display information about their internal processes required for creating a new Cisco Webex Messenger account.

For example:

To obtain the Cisco Webex Messenger service, send an email to ithelpdesk@mycompany.com, or call +1 800 555 5555.

Enter User Provisioning Information

Procedure

Step 1 To enter user provisioning information, under the **Configuration** tab select **System Settings** > **User Provisioning**.

Step 2 To enable users to self-register for an account with the Cisco Jabber application, select **Enable user self-registration using** Cisco Webex **registration page**.

The URL for the self-registration page is www.webex.com/go/wc. The Cisco Webex Messenger organization Administrator typically provides this URL.

Note If you do not select Enable user self-registration using Cisco Webex registration page, the Custom Registration URL field and the Custom Message box is displayed. In this case, you will need to enter the URL for the custom user registration page.

Step 3 In the **Custom Registration URL** field, enter the URL of the customized self-registration page.

If you do not enter a custom URL, the following self-registration page (default) URL is displayed: www.webex.com/go/wc.

Step 4 In the **Custom Message** box, enter a description for the custom self-registration page.

Step 5 To notify the Organization Administrator via email each time a user registers using the self-registration page, select **Send notification to Administrator when users self register using Cisco Webex registration page**.

Step 6 Under **Set mandatory fields for user profile**, select the fields that are compulsorily displayed each time a user's profile is created or viewed. These fields always appear each time you:

- create a new user
- edit an existing user profile
- import users from a CSV file

Step 7 Select **Save**.

Create and Import a CSV File

You can easily import a large number of users from a comma separated values (CSV) file into your Cisco Webex Messenger organization. Similarly, you can export your users to a CSV file. Importing is a useful way of painlessly adding a large number of users to your organization thereby saving the effort of manually adding each user.

After the import is complete, the Organization Administrator who initiated the import receives an email with the status of the import. The email states whether the import was a success, failure, or terminated.

The CSV file is imported and the users appear in the **User** tab.

CSV Fields

Note: Organization Administrators and User Administrators cannot be created using the CSV Import process.

The following fields (in no specific order) should be included in the CSV file prior to importing users into Cisco Webex. Some fields are mandatory, you must enter information into them, and some are optional.

Note: If you do not want to enter information into a field, you can enter the character "-" and it is imported into the database as an empty field. You can only do this for optional fields. If you input "-" in a mandatory field, an error is reported on import. Do not use the value N/A.

Field Name	Description
employeeID	*Mandatory (only SSO enabled)* Enter the user's ID.
displayName	*Optional* Enter the user's display name.
firstName	*Mandatory* Enter the user's first name.
lastName	*Mandatory* Enter the user's last name.
email	*Mandatory* Enter the user's email address.
userName	*Mandatory* Enter the user's username in the user@email.com format.
jobTitle	*Optional* Enter the user's job title or designation.
address1	*Optional* Enter the first line of the user's address. The Organization Administrator can configure this field so that it is mandatory for users.
address2	*Optional* Enter the second line of the user's address. The Organization Administrator can configure this field so that it is mandatory for users.
city	*Optional* Enter the city in which the user lives. The Organization Administrator can configure this field so that it is mandatory for users.

Field Name	Description
state	*Optional* Enter the state in which the user lives. The Organization Administrator can configure this field so that it is mandatory for users.
zipCode	*Optional* Enter the user's ZIP code. The Organization Administrator can configure this field so that it is mandatory for users.
ISOcountry	*Optional* Enter the two letter country code, for example IN, US, CN, in which the user lives. For more information see http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm. The Organization Administrator can configure this field so that it is mandatory for users.
phoneBusinessISOCountry	*Optional* Enter the country code, for example IN, US, CN, for the user's business phone number. The Organization Administrator can configure this field so that it is mandatory for users.
phoneBusinessNumber	*Optional* Enter the user's business phone number. The Organization Administrator can configure this field so that it is mandatory for users.
phoneMobileISOCountry	*Optional* Enter the country code, for example IN, US, CN, for the user's mobile phone number. The Organization Administrator can configure this field so that it is mandatory for users.
phoneMobileNumber	*Optional* Enter the user's mobile phone number. The Organization Administrator can configure this field so that it is mandatory for users.
fax	*Optional* Enter the user's fax number.
policyGroupName	*Optional* Enter the default policy group to which the user belongs.
userProfilePhotoURL	*Optional* Enter the URL where the user's profile picture can be accessed.
activeConnect	*Optional* Indicate whether the user's status is **active** in Cisco Webex Enter **Yes** to indicate an **active** status and **No** to indicate an **inactive** status.
center	*Optional* Used to assign (Yes) or remove (No) the center account for the Cisco Jabber application user. Only one center can be specified.

Field Name	Description
storageAllocated	*Optional* Enter the storage allocated to the user in Megabytes. This must be a numerical value
CUCMClusterName	*Optional* Enter the name of the Cisco Unified Communications Manager cluster that the user belongs to.
businessUnit	*Optional* Enter the business unit or department of the user. The Organization Administrator can configure this field so that it is mandatory for users.
IMLoggingEnable	*Optional* Indicate if IM logging is enabled for this user. Enter **True** to indicate an **enabled** status and **False** to indicate a **disabled** status.
endpointName	*Optional* Enter the endpoint name configured for logging IMs.
autoUpgradeSiteName	*Optional* Enter the upgrade site name.

Note You can use tab, or comma-separated CSV files. Ensure that your CSV file is encoded in either UTF-8 or UTF16-LE formats.

Select UTF-8 as the Encoding Format

Procedure

Step 1 In Microsoft Excel select **File > Save As**.

Step 2 In the **Save As** dialog box, select **Tools and Web Options**.

Step 3 In the **Web Options** dialog box, select the **Encoding** tab.

Step 4 From the **Save this document as** list, **select UTF-8**.

Step 5 Select **OK** to return to the **Save As** dialog box.

Step 6 From the **Save as type** list, select **CSV (Comma delimited) (*.csv)**.

Step 7 In the **File Name** field, type a name for the CSV file and select **Save**.

Import and Export Users

Procedure

Step 1 To import users from a CSV file, in the Cisco Webex Messenger Administration Tool, select the **User tab** > **More Actions > Import/Export**.

Step 2 Select **Browse** and select the CSV file that contains the list of users you want to import.

Step 3 Select **Import** to begin the import process.

Step 4 To export users, select **Export** in the **Import/Export User** dialog box.

A progress message indicates the progress of the export process.

Step 5 To view the CSV file that contains the exported users, select the time stamp of the export message. A confirmation prompt appears. The message resembles the following example: `Last export: 2009-06-24 09:02:01`.

Step 6 Select **Open** to view the CSV file containing your Messenger organization's users. Alternatively, select **Save** to save the CSV file to your local computer.

Assign Users to Policies

Procedure

Step 1 To assign users to policy groups, select the **User tab**.

Step 2 If you want to assign a policy group to a new user, create the new user first by selecting **Add**.

Step 3 If you want to assign a policy group to an existing user, search for the user.

Step 4 In the search result, double-click the appropriate user's name to open the **Edit User** dialog box.

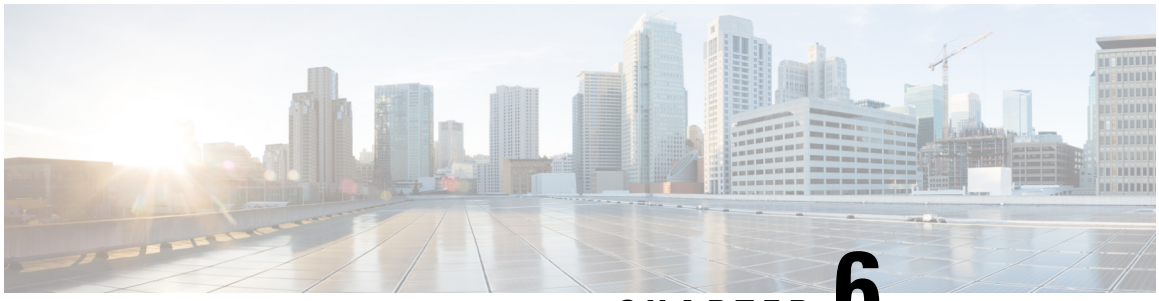
Step 5 Select the **Policy Group Assignment tab** to open the **Policy Group Assignment** dialog box.

Step 6 In the **Search** field, enter at least one letter of the policy group that you want to search for and assign to this user.

Step 7 Select **Search.**

Step 8 In the **Search Result** window, select the appropriate policy group and select **Assign** to assign the policy to this user.

Step 9 Select **Save** to save the policy group assignment and return to the **User** tab.



CHAPTER 6

Create Users for Hybrid Deployment

Enable Synchronization

To ensure that contact data in your directory server is replicated to Cisco Unified Communications Manager, you must synchronize with the directory server. Before you can synchronize with the directory server, you must enable synchronization.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **LDAP** > **LDAP System**.

The **LDAP System Configuration** window opens.

Step 3 Locate the **LDAP System Information** section.

Step 4 Select **Enable Synchronizing from LDAP Server**.

Step 5 Select the type of directory server from which you are synchronizing data from the **LDAP Server Type** drop-down list.

What to do next

Specify an LDAP attribute for the user ID.

Specify an LDAP Attribute for the User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, you can populate the user ID from an attribute in the directory. The default attribute that holds the user ID is `sAMAccountName`.

Procedure

Step 1 Locate the **LDAP Attribute for User ID** drop-down list on the **LDAP System Configuration** window.

Step 2 Specify an attribute for the user ID as appropriate and then select **Save**.

Important If the attribute for the user ID is other than `sAMAccountName` and you are using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The CDI parameter is `UserAccountName`.

`<UserAccountName>`*`attribute-name`*`</UserAccountName>`

If you do not specify the attribute in your configuration, and the attribute is other than `sAMAccountName`, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager release 9.0(1) and later, you can populate the directory URI from an attribute in the directory.

Before you begin

Enable Synchronization.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select the appropriate LDAP directory or select **Add New** to add an LDAP directory.

Step 3 Locate the **Standard User Fields To Be Synchronized** section.

Step 4 Select one of the following LDAP attributes from the **Directory URI** drop-down list:

- **msRTCSIP-primaryuseraddress**—This attribute is populated in the AD when Microsoft Lync or Microsoft OCS are used. This is the default attribute.
- **mail**

Step 5 Select **Save**.

Perform Synchronization

After you add a directory server and specify the required parameters, you can synchronize Cisco Unified Communications Manager with the directory server.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select **Add New**.

The **LDAP Directory** window opens.

Step 3 Specify the required details on the **LDAP Directory** window.

See the Cisco Unified Communications Manager Administration Guide for more information about the values and formats you can specify.

Step 4 Create an LDAP Directory Synchronization Schedule to ensure that your information is synchronized regularly.

Step 5 Select **Save**.

Step 6 Select **Perform Full Sync Now**.

Note The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.

User data from your directory server is synchronized to the Cisco Unified Communications Manager database. Cisco Unified Communications Manager then synchronizes the user data to the presence server database.

Assign Roles and Groups

For all deployment types assign users to the **Standard CCM End Users** group.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**
The **Find and List Users** window opens.

Step 3 Find and select the user from the list.
The **End User Configuration** window opens.

Step 4 Locate the **Permission Information** section.

Step 5 Select **Add to Access Control Group**.

The **Find and List Access Control Groups** dialog box opens.

Step 6 Select the access control groups for the user.

At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**—This option is used for desk phone control.

If you provision users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 7 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 8 Select **Save** on the **End User Configuration** window.

Authentication Options

Enable SAML SSO in the Client

Before you begin

- If you do not use Cisco Webex Messenger, enable SSO on Cisco Unified Communications Applications 10.5.1 Service Update 1—For information about enabling SAML SSO on this service, read the *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*.
- Enable SSO on Cisco Unity Connection version 10.5—For more information about enabling SAML SSO on this service, read *Managing SAML SSO in Cisco Unity Connection*.
- If you use Cisco Webex Messenger, enable SSO on Cisco Webex Messenger Services to support Cisco Unified Communications Applications and Cisco Unity Connection—For more information about enabling SAML SSO on this service, read about *Single Sign-On* in the *Cisco Webex Messenger Administrator's Guide*.

  For more information about enabling SAML SSO on this service, read about `Single Sign-On` in the *Cisco Webex Messenger Administrator's Guide*.

Procedure

Step 1 Deploy certificates on all servers so that the certificate can be validated by a web browser, otherwise users receive warning messages about invalid certificates. For more information about certificate validation, see *Certificate Validation*.

Step 2 Ensure Service Discovery of SAML SSO in the client. The client uses standard service discovery to enable SAML SSO in the client. Enable service discovery by using the following configuration parameters: ServicesDomain,VoiceServicesDomain, and ServiceDiscoveryExcludedServices. For more information about how to enable service discovery, see *Configure Service Discovery for Remote Access*.

Step 3 Define how long a session lasts.

A session is comprised of cookie and token values. A cookie usually lasts longer than a token. The life of the cookie is defined in the Identity Provider, and the duration of the token is defined in the service.

Step 4 When SSO is enabled, by default all Cisco Jabber users sign in using SSO. Administrators can change this on a per user basis so that certain users do not use SSO and instead sign in with their Cisco Jabber username and password. To disable SSO for a Cisco Jabber user, set the value of the SSO_Enabled parameter to FALSE.

If you have configured Cisco Jabber not to ask users for their email address, their first sign in to Cisco Jabber may be non-SSO. In some deployments, the parameter ServicesDomainSsoEmailPrompt needs to be set to ON. This ensures that Cisco Jabber has the information required to perform a first-time SSO sign in. If users signed in to Cisco Jabber previously, this prompt is not needed because the required information is available.

Authenticate with the LDAP Server

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords. When users sign in to the client, the presence service routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then sends that authentication to the directory server.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

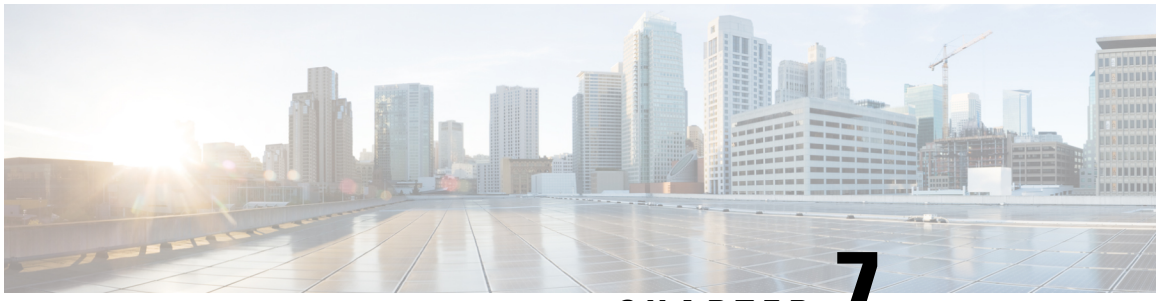
Step 2 Select **System** > **LDAP** > **LDAP Authentication**.

Step 3 Select **Use LDAP Authentication for End Users**.

Step 4 Specify LDAP credentials and a user search base as appropriate.

See the *Cisco Unified Communications Manager Administration Guide* for information about the fields on the **LDAP Authentication** window.

Step 5 Select **Save**.



CHAPTER 7

Configure Deskphone Control

Prerequisites

The Cisco CTIManager service must be running in the Cisco Unified Communications Manager cluster.

Configure Deskphone Control Taskflow

Procedure

	Command or Action	Purpose
Step 1	Enable Device for CTI, on page 30	Allows Cisco Jabber desktop clients to control the desk phone of the user.
Step 2	Configure Desk Phone Video, on page 30.	Let users receive video transmitted to their desk phone devices on their computers through the client.
Step 3	Enable Video Rate Adaptation, on page 31	The client uses video rate adaptation to negotiate optimum video quality.
Step 4	Configure User Associations, on page 33	Associate users with devices and assign users to access control groups.
Step 5	Reset Devices, on page 34	You must reset devices after you configure user associations.

Enable Device for CTI

If you want Cisco Jabber desktop clients to be able to control the desk phone of the user, you must select the **Allow Control of Device from CTI** option when you create the device for the user.

Procedure

Step 1 In Cisco Unified CM Administration, click **Device** > **Phone** and search for the phone.

Step 2 In the **Device Information** section, check **Allow Control of Device from CTI**.

Step 3 Click **Save**.

Configure Desk Phone Video

Desk phone video capabilities let users receive video transmitted to their desk phone devices on their computers through the client. Users must physically connect the computer to the desk phone device through the computer port so that the client can establish a connection to the device. Users cannot use desk phone video capabilities with wireless connections to desk phone devices.

Note If users have both wireless and wired connections available, they should configure Microsoft Windows so that wireless connections do not take priority over wired connections. See the following Microsoft documentation for more information: *An explanation of the Automatic Metric feature for Internet Protocol routes*.

For desk phone video capabilities, you must download and install Jabber Desk Phone Video Services Interface from Cisco.com. Jabber Desk Phone Video Services Interface provides the Cisco Discover Protocol (CDP) driver that enables the client to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

Desk Phone Video Considerations

Review the following considerations and limitations before you provision desk phone video capabilities for users:

- You cannot use desk phone video capabilities on devices if video cameras are attached to the devices, such as a Cisco Unified IP Phone 9971. You can use desk phone video capabilities if you remove video cameras from the devices.
- You cannot use desk phone video capabilities with devices that do not support CTI.
- Video desktop sharing, using the BFCP protocol, is not supported with desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send video result in audio only calls.

- 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.
- If a user initiates a call from the keypad on a desk phone device, the call starts as an audio call on the desk phone device. The client then escalates the call to video. For this reason, you cannot make video calls to devices that do not support escalation, such as H.323 endpoints. To use desk phone video capabilities with devices that do not support escalation, users should initiate calls from the client.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. You must upgrade your firmware to version SCCP45.9-3-1 to use desk phone video capabilities.
- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets, which disables desk phone video capabilities. You should configure your antivirus or firewall application to allow inbound CDP packets.

  See the following Symantec technical document for additional details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.
- You must not select the **Media Termination Point Required** checkbox on the SIP trunk configuration for Cisco Unified Communications Manager. Desk phone video capabilities are not available if you select this checkbox.

Procedure

Step 1 Physically connect the computer to the computer port on the desk phone device.

Step 2 Enable the desk phone device for video in Cisco Unified Communications Manager.

Step 3 Install Jabber Desk Phone Video Services Interface on the computer.

Troubleshooting Desk Phone Video

If you encounter an error that indicates desk phone video capabilities are unavailable or the desk phone device is unknown, do the following:

1. Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.
2. Reset the physical desk phone.
3. Exit the client.
4. Run services.msc on the computer where you installed the client.
5. Restart Jabber Desk Phone Video Services Interface from the Services tab of the Windows Task Manager.
6. Restart the client.

Enable Video Rate Adaptation

The client uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video quality based on network conditions.

To use video rate adaptation, you must enable Real-Time Transport Control Protocol (RTCP) on Cisco Unified Communications Manager.

Note RTCP is enabled on software phone devices by default. However, you must enable RTCP on desk phone devices.

Enable RTCP on Common Phone Profiles

You can enable RTCP on a common phone profile to enable video rate adaptation on all devices that use the profile.

Note RTCP is an integral component of Jabber Telephony services. Jabber will continue to send RTCP packets even when disabled.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.

The **Find and List Common Phone Profiles** window opens.

Step 3 Specify the appropriate filters in the **Find Common Phone Profile where** field and then select **Find** to retrieve a list of profiles.

Step 4 Select the appropriate profile from the list.

The **Common Phone Profile Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Enable RTCP on Device Configurations

You can enable RTCP on specific device configurations instead of a common phone profile. The specific device configuration overrides any settings you specify on the common phone profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of phones.

Step 4 Select the appropriate phone from the list.

The **Phone Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.

The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.

The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section.

Step 6 Select **Home Cluster**.

Step 7 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

Step 8 Locate the **Device Information** section.

Step 9 Select **Device Association**.

The **User Device Association** window opens.

Step 10 Select the devices to which you want to associate the user. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a user.

Step 11 Select **Save Selected/Changes**.

Step 12 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 13 Find and select the same user from the list.

The **End User Configuration** window opens.

Step 14 Locate the **Permissions Information** section.

Step 15 Select **Add to Access Control Group**.

The **Find and List Access Control Groups** dialog box opens.

Step 16 Select the access control groups to which you want to assign the user.

At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 17 Select **Add Selected**.

The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.

Reset Devices

After you create and associate users with devices, you should reset those devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

Step 4 Select the appropriate device from the list.

The **Phone Configuration** window opens.

Step 5 Locate the **Association Information** section.

Step 6 Select the appropriate directory number configuration.

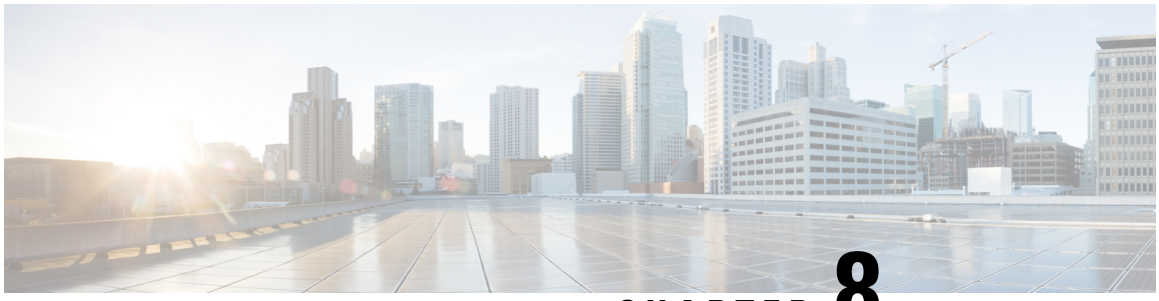
The **Directory Number Configuration** window opens.

Step 7 Select **Reset**.

The **Device Reset** dialog box opens.

Step 8 Select **Reset**.

Step 9 Select **Close** to close the **Device Reset** dialog box.



CHAPTER 8

Configure Softphone

Create Softphones Workflow

Procedure

	Command or Action	Purpose
Step 1	Create and Configure Cisco Jabber Devices, on page 35	Create at least one device for every user that will access Cisco Jabber. Generate an authentication string to provide to end users.
Step 2	Add a Directory Number to the Device, on page 39	For each device you create, add a directory number.
Step 3	Associate Users with Devices, on page 39	Associate users with devices.
Step 4	Create Mobile SIP Profiles, on page 40.	Complete this task if you have Cisco Unified Communications Manager release 9 and plan to configure devices for mobile clients.
Step 5	Configure the Phone Security Profile, on page 41	Complete this task to set up secure phone capabilities for all devices.

Create and Configure Cisco Jabber Devices

Create at least one device for every user that accesses Cisco Jabber. A user can have multiple devices.

Note Users can only remove participants from a conference call when using the softphone (CSF) device for calls.

Before you begin

- Install COP files.

- Create SIP profiles if you have Cisco Unified Communications Manager release 9 or earlier and plan to configure devices for mobile clients.
- Create the Phone Security Profile if you plan to set up secure phone capabilities for all devices.
- If you are using CAPF enrollment, for Cisco Unified Communications Manager release 10 or later, ensure that the Cisco Certificate Authority Proxy Function (CAPF) service parameters value for **Certificate Issuer to Endpoint** is **Cisco Certificate Authority Proxy Function**. This is the only option supported by Cisco Jabber. For information on configuring the CAPF service parameter see the *Update CAPF Service Parameters* topic in the Cisco Unified Communications Manager Security Guides.
- Before you create TCT devices, BOT devices, or TAB devices for Cisco Jabber for mobile users, specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In Unified CM Administration interface, select **System** > **Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com. This top domain name is used by Jabber as the DNS domain of the Cisco Unified Communications Manager servers for phone registration. For example, CUCMServer1@cisco.com.

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
Find and List Phones window opens.

Step 3 Select **Add New**.

Step 4 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

For Jabber users, you can only create one type of device per user although you can create multiple devices for each user. For example, you can create one tablet device and one CSF device but not two CSF devices.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TCT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.

Step 5 From the **Owner User ID** drop-down list, select the user for whom you want to create the device.

For the **Cisco Unified Client Services Framework** option in a Phone mode deployment, ensure that **User** is selected.

Step 6 In the **Device Name** field, use the applicable format to specify a name for the device:

If You Select	Required Format
Cisco Unified Client Services Framework	• Valid characters: a–z, A–Z, 0–9. • 15-character limit.

If You Select	Required Format
Cisco Dual Mode for iPhone	• The device name must begin with *TCT*. For example, if you create a TCT device for user, Tanya Adams, whose username is tadams, enter **TCTTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Jabber for Tablet	• The device name must begin with *TAB*. For example, if you create a TAB device for user, Tanya Adams, whose username is tadams, enter **TABTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Dual Mode for Android	• The device name must begin with *BOT*. For example, if you create a BOT device for user, Tanya Adams, whose username is tadams, enter **BOTTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.

Step 7 If you are using CAPF enrollment, complete the following steps to generate an authentication string:

1. Users can use the authentication string that you can provide to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.
2. From the **Certificate Operation** drop-down list, select **Install/Upgrade**.
3. From the **Authentication Mode** drop-down list, select **By Authentication String** or **By Null String**. Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.
4. Click **Generate String**. The Authentication String autopopulates with a string value. This is the string that you will provide to end users.
5. From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.

6. In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.
7. If you are using a group configuration file, specify it in the **Cisco Support Field** of the **Desktop Client Settings.** Cisco Jabber does not use any other settings that are available on the **Desktop Client Settings**.

Step 8 Select **Save**.

Step 9 Click **Apply Config**.

What to do next

Add a Directory Number to the device.

Provide Users with Authentication Strings

If you are using CAPF enrollment to configure secure phones, then you must provide users with authentication strings. Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.

Note The time it takes for the enrollment process to complete can vary depending on the user's computer or mobile device and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

  In this case, you must generate a new authentication string on the user's device. The user must then enter that authentication string before the expiration time.

Important When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the Standard CTI Secure Connection user group.

Add a Directory Number to the Device

After you create and configure each device, you must add a directory number to the device. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option.

Before you begin

Create a device.

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.
Step 2 Click **Add a new DN**.
Step 3 In the **Directory Number** field, specify a directory number.
Step 4 In the **Users Associated with Line** section, click **Associate End Users**.
Step 5 In the **Find User where** field, specify the appropriate filters and then click **Find**.
Step 6 From the list that appears, select the applicable users and click **Add Selected**.
Step 7 Specify all other required configuration settings as appropriate.
Step 8 Select **Apply Config**.
Step 9 Select **Save**.

Associate Users with Devices

On Cisco Unified Communications Manager version 9.x only, when the client attempts to retrieve the service profile for the user, it first gets the device configuration file from Cisco Unified Communications Manager. The client can then use the device configuration to get the service profile that you applied to the user.

For example, you provision Adam McKenzie with a CSF device named `CSFAKenzi`. The client retrieves `CSFAKenzi.cnf.xml` from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in `CSFAKenzi.cnf.xml`:

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

For this reason, if you are using Cisco Unified Communications Manager version 9.x, you should do the following to ensure that the client can successfully retrieve the service profiles that you apply to users:

- Associate users with devices.
- Set the **User Owner ID** field in the device configuration to the appropriate user. The client will retrieve the Default Service Profile if this value is not set.

Note A CSF should not be associated to multiple users if you intend to use different service profiles for these users.

Procedure

Step 1 Associate users with devices.

a) Open the **Unified CM Administration** interface.
b) Select **User Management** > **End User**.
c) Find and select the appropriate user.
The **End User Configuration** window opens.
d) Select **Device Association** in the **Device Information** section.
e) Associate the user with devices as appropriate.
f) Return to the **End User Configuration** window and then select **Save**.

Step 2 Set the **User Owner ID** field in the device configuration.

a) Select **Device** > **Phone**.
b) Find and select the appropriate device.
The **Phone Configuration** window opens.
c) Locate the **Device Information** section.
d) Select **User** as the value for the **Owner** field.
e) Select the appropriate user ID from the **Owner User ID** field.
f) Select **Save**.

Create Mobile SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients. Before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communication Manager Release 10, choose the **Standard SIP Profile for Mobile Device** default profile when you create and configure devices for mobile clients.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.

The **Find and List SIP Profiles** window opens.

Step 3 Do one of the following to create a new SIP profile:

- Find the default SIP profile and create a copy that you can edit.
- Select **Add New** and create a new SIP profile.

Step 4 In the new SIP profile, set the following values:

- **Timer Register Delta** = 120
- **Timer Register Expires** = 720

- **Timer Keep Alive Expires** = 720
- **Timer Subscribe Expires** = 21600
- **Timer Subscribe Delta** = 15

Step 5 Select **Save**.

Setting up System SIP Parameters

If you are connected to a low-bandwidth network and finding it difficult to take an incoming call on your mobile device, you can set the system SIP parameters to improve the condition. Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before you begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **Service Parameters**.

Step 3 Select the node.

Step 4 Select the **Cisco CallManager (Active)** service.

Step 5 Scroll to the **Clusterwide Parameters (System - Mobility)** section.

Step 6 Increase the **SIP Dual Mode Alert Timer** value to 10000 milliseconds.

Step 7 Select **Save**.

Note If, after you increase the SIP Dual Mode Alert Timer value, incoming calls that arrive in Cisco Jabber are still terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value again in increments of 500 milliseconds.

Configure the Phone Security Profile

You can optionally set up secure phone capabilities for all devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection.

Before you begin

- Configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. At minimum, select mixed mode security.

For instructions on how to configure mixed mode with the Cisco CTL Client, see the Cisco Unified Communications Manager Security Guide.

- For conference calls, ensure that the conferencing bridge supports secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

Procedure

Step 1 In **Cisco Unified Communications Manager**, select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TFT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.
- **CTI Remote Device**—Select this option to create a CTI remote device.

  CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Step 4 In the **Name** field of the **Phone Security Profile Configuration** window, specify a name for the phone security profile.

Step 5 For **Device Security Mode**, select one of the following options:

- **Authenticated**—The SIP connection is over TLS using NULL-SHA encryption.
- **Encrypted**—The SIP connection is over TLS using AES 128/SHA encryption. The client uses Secure Real-time Transport Protocol (SRTP) to offer encrypted media streams.

Step 6 For **Transport Type**, leave the default value of **TLS**.

Step 7 Select the **TFTP Encrypted Config** check box to encrypt the device configuration file that resides on the TFTP server.

Note For a TCT/BOT/Tablet device, do not select the TFTP Encrypted Config check box here. For Authentication Mode, select By Authentication String or Null String.

Step 8 For **Authentication Mode**, select **By Authentication String** or **By Null String**.

Note Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.

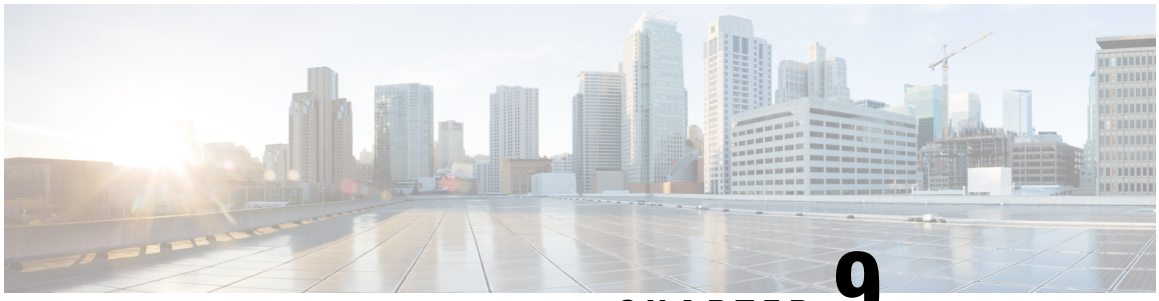
Step 9 For **Key Size (Bits)**, select the appropriate key size for the certificate. Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

The Cisco Jabber clients were tested using authentication strings with 1024-bit length keys. The Cisco Jabber clients require more time to generate 2048-bit length keys than 1024-bit length keys. As a result, if you select 2048, expect it to take longer to complete the CAPF enrollment process.

Step 10 For **SIP Phone Port**, leave the default value.

The port that you specify in this field takes effect only if you select **Non Secure** as the value for **Device Security Mode**.

Step 11 Click **Save**.



CHAPTER 9

Configure Extend and Connect

Configure Extend and Connect Workflow

Procedure

	Command or Action	Purpose
Step 1	Enable User Mobility, on page 45	Enable users mobility and you can assign users as owners of CTI remote devices.
Step 2	Create CTI Remote Devices, on page 46	Create CTI remote devices, these virtual devices monitor and have call control over a user's remote destination.
Step 3	Add a Remote Destination, on page 47	(Optional) If you plan to provision users with dedicated CTI remote devices, add a remote destination in Cisco Unified Communications Manager.

Enable User Mobility

This task is only for desktop clients.

You must enable user mobility to provision CTI remote devices. If you do not enable mobility for users, you cannot assign those users as owners of CTI remote devices.

Before you begin

This task is applicable only if:

- You plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.

- You have Cisco Unified Communication Manager release 9.x and later.

Procedure

Step 1 Select **User Management** > **End User**.

The **Find and List Users** window opens.

Step 2 Specify the appropriate filters in the **Find User where** field to and then select **Find** to retrieve a list of users.

Step 3 Select the user from the list.

The **End User Configuration** window opens.

Step 4 Locate the **Mobility Information** section.

Step 5 Select **Enable Mobility**.

Step 6 Select **Save**.

Create CTI Remote Devices

CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select **CTI Remote Device** from the **Phone Type** drop-down list and then select **Next**.

The **Phone Configuration** window opens.

Step 5 Select the appropriate user ID from the **Owner User ID** drop-down list.

Note Only users for whom you enable mobility are available from the **Owner User ID** drop-down list. For more information, see Enable SAML SSO in the Client.

Cisco Unified Communications Manager populates the **Device Name** field with the user ID and a **CTIRD** prefix; for example, **CTIRDusername**

Step 6 Edit the default value in the **Device Name** field, if appropriate.

Step 7 Ensure you select an appropriate option from the **Rerouting Calling Search Space** drop-down list in the **Protocol Specific Information** section.

The **Rerouting Calling Search Space** drop-down list defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.

Step 8 Specify all other configuration settings on the **Phone Configuration** window as appropriate.

See the *CTI remote device setup* topic in the System Configuration Guide for Cisco Unified Communications Manager documentation for more information.

Step 9 Select **Save**.

The fields to associate directory numbers and add remote destinations become available on the **Phone Configuration** window.

Add a Remote Destination

Remote destinations represent the CTI controllable devices that are available to users.

You should add a remote destination through the **Cisco Unified CM Administration** interface if you plan to provision users with dedicated CTI remote devices. This task ensures that users can automatically control their phones and place calls when they start the client.

If you plan to provision users with CTI remote devices along with software phone devices and desk phone devices, you should not add a remote destination through the **Cisco Unified CM Administration** interface. Users can enter remote destinations through the client interface.

Note

- You should create only one remote destination per user. Do not add two or more remote destinations for a user.
- Cisco Unified Communications Manager does not verify if it can route remote destinations that you add through the **Cisco Unified CM Administration** interface. For this reason, you must ensure that Cisco Unified Communications Manager can route the remote destinations you add.
- Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field to and then select **Find** to retrieve a list of phones.

Step 4 Select the CTI remote device from the list.

The **Phone Configuration** window opens.

Step 5 Locate the **Associated Remote Destinations** section.

Step 6 Select **Add a New Remote Destination**.

The **Remote Destination Information** window opens.

Step 7 Specify JabberRD in the **Name** field.

Restriction You must specify JabberRD in the **Name** field. The client uses only the JabberRD remote destination. If you specify a name other than JabberRD, users cannot access that remote destination.

The client automatically sets the JabberRD name when users add remote destinations through the client interface.

Step 8 Enter the destination number in the **Destination Number** field.

Step 9 Specify all other values as appropriate.

Step 10 Select **Save**.

What to do next

Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

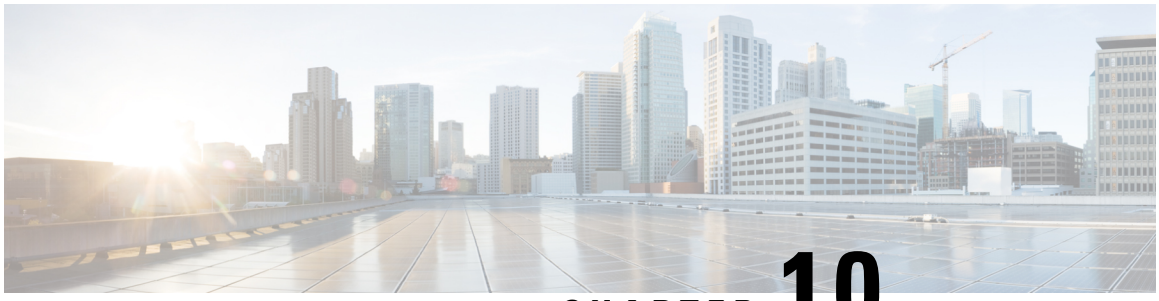
1. Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
2. Locate the **Associated Remote Destinations** section.
3. Verify the remote destination is available.
4. Select **Apply Config**.

Note The **Device Information** section on the **Phone Configuration** window contains a **Active Remote Destination** field.

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**.

none displays as the value of **Active Remote Destination** if:

- Users do not select a remote destination in the client.
- Users exit or are not signed in to the client.



CHAPTER 10

Configure Service Discovery for Remote Access

Service Discovery Requirements

Service discovery enables clients to automatically detect and locate services on your enterprise network. Expressway for Mobile and Remote Access allows you to access the services on your enterprise network. You should meet the following requirements to enable the clients to connect through Expressway for Mobile and Remote Access and discover services:

- DNS requirements
- Certificate requirements
- Test external SRV `_collab-edge`.

DNS Requirements

The DNS requirements for service discovery through remote access are:

- Configure a `_collab-edge` DNS SRV record on an external DNS server.
- Configure a `_cisco-uds` DNS SRV record on the internal name server.
- Optionally, for a hybrid cloud-based deployment with different domains for the IM and Presence server and the voice server, configure the Voice Services Domain to locate the DNS server with the `_collab-edge` record.

Note Jabber attempts connections to a maximum of three SSO-enabled servers, which are chosen randomly from all SSO-enabled servers that the DNS SRV records (`_collab-edge` and `_cisco-uds`) identify. If Jabber fails to connect three times, it considers Edge SSO unsupported.

Certificate Requirements

Before you configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.

For more information on configuring Cisco VCS Expressway certificate, see Configuring Certificates on Cisco VCS Expressway.

Test _collab-edge SRV Record

Procedure

Step 1 Open a command prompt.

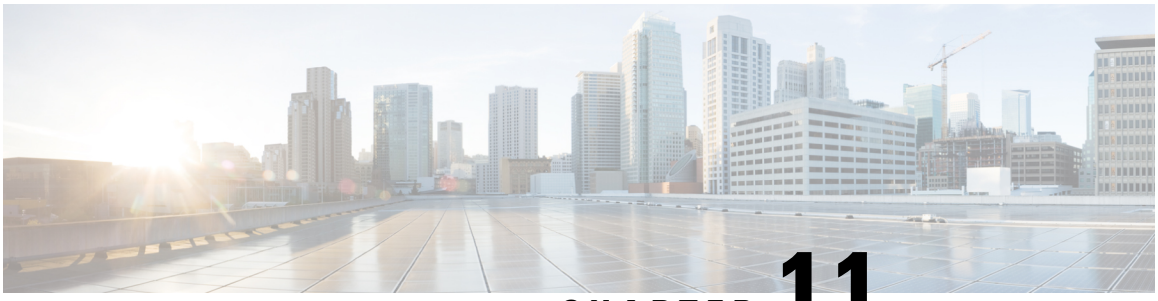
Step 2 Enter **nslookup**.
The default DNS server and address is displayed. Confirm that this is the expected DNS server.

Step 3 Enter **set type=SRV**.

Step 4 Enter the name for each of your SRV records.

For example `_collab-edge.`*`exampledomain`*

- Displays server and address—SRV record is accessible.
- Displays `_collab-edge.`*`exampledomain`*`: Non-existent domain`—There is an issue with your SRV record.



CHAPTER 11

Set Up Certificate Validation

Certificate Validation for Cloud Deployments

Cisco Webex Messenger and Cisco Webex Meetings Center present the following certificates to the client by default:

- CAS
- WAPI

Note Cisco Webex certificates are signed by a public Certificate Authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

Cisco Jabber validates the following XMPP certificates received from Cisco Webex Messenger. If these certificates are not included in your operating system, you must provide them.

- VeriSign Class 3 Public Primary Certification Authority - G5 — This certificate is stored in the Trusted Root Certificate Authority
- VeriSign Class 3 Secure Server CA - G3 —This certificate validates the Webex Messenger server identity and is stored in the Intermediate Certificate Authority.
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority Root Certificate

For more information about root certificates for Cisco Jabber for Windows, see https://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For more information about root certificates for Cisco Jabber for Mac, see https://support.apple.com.

Update Profile Photo URLs

In cloud-based deployments, Cisco Webex assigns unique URLs to profile photos when you add or import users. When Cisco Jabber resolves contact information, it retrieves the profile photo from Cisco Webex at the URL where the photo is hosted.

Profile photo URLs use HTTP Secure (`https://server_name/`) and present certificates to the client. If the server name in the URL is:

- A fully qualified domain name (FQDN) that contains the Cisco Webex domain — The client can validate the web server that is hosting the profile photo against the Cisco Webexcertificate.
- An IP address — The client cannot validate the web server that is hosting the profile photo against the Cisco Webex certificate. In this case, the client prompts users to accept certificates whenever they look up contacts with an IP address in their profile photo URLs.

Important

- We recommend that you update all profile photo URLs that contain an IP address as the server name. Replace the IP address with the FQDN that contains the Cisco Webex domain to ensure that the client does not prompt users to accept certificates.
- When you update a photo, the photo can take up to 24 hours to refresh in the client.

The following steps describe how to update profile photo URLs. Refer to the appropriate Cisco Webex documentation for detailed instructions.

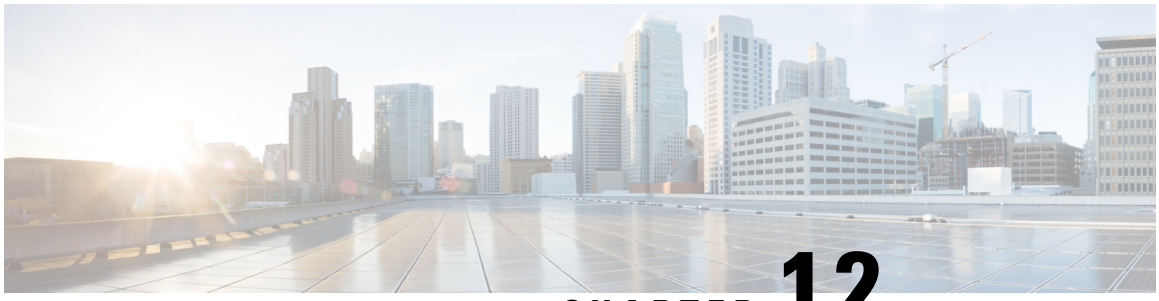
Procedure

Step 1 Export user contact data in CSV file format with the Cisco WebexAdministration Tool.

Step 2 In the **userProfilePhotoURL** field, replace IP addresses with the Cisco Webex domain.

Step 3 Save the CSV file.

Step 4 Import the CSV file with the Cisco Webex Administration Tool.



CHAPTER 12

Configure the Clients

Client Configuration Workflow

Procedure

	Command or Action	Purpose
Step 1	Introduction to Client Configuration, on page 53	
Step 2	Create and Host Client Configuration Files Using an XML Editor, on page 54	
Step 3	Set Parameters on Phone Configuration for Desktop Clients, on page 58	
Step 4	Set Parameters on Phone Configuration for Mobile Clients, on page 60	
Step 5	Configure Proxy Setting, on page 60	

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

- Service Profiles—You can configure some client settings in UC service profiles on Cisco Unified Communications Manager release 9 and later. When users launch the client, it discovers the Cisco Unified Communications Manager home cluster using a DNS SRV record and automatically retrieves the configuration from the UC service profile.

  Applies to on-premises deployments only.

- Phone Configuration—You can set some client settings in the phone configuration on Cisco Unified Communications Manager release 9 and later. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.

  Applies to on-premises deployments only.

- Cisco Unified Communications Manager IM and Presence Service—You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

  In the **Advanced settings** window, if you select **Cisco IM & Presence**, the client retrieves UC services from Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.

  Applies to on-premises deployments only.

- Client Configuration Files—You can create XML files that contain configuration parameters. You then host the XML files on a TFTP server. When users sign in, the client retrieves the XML file from the TFTP server and applies the configuration.

  Applies to on-premises and cloud-based deployments.

- Cisco Webex Administration Tool—You can configure some client settings with the Cisco Webex Administration Tool.

  You can upload a `jabber-config.xml` client configuration file into the Cisco Webex Administration Tool. You can apply separate configuration files for groups in the Cisco Webex Messenger Administration Tool. When the client successfully connects to Cisco Webex Messenger it downloads the XML file and the configuration is applied.

  The client will use the following order for configuration settings:

  1. Settings in Cisco Webex Messenger Administration Tool
  2. Settings in `jabber-config.xml` file from Cisco Webex Messenger Administration Tool.

     Note Group configuration file settings take priority over the configuration file in Cisco Webex Messenger Administration Tool.

  3. Settings in `jabber-config.xml` file from the TFTP server.

  If there are any conflicts with configuration settings, the settings set in Cisco Webex Administration tool will take priority over this configuration file.

  Applies to cloud-based deployments only.

Create and Host Client Configuration Files Using an XML Editor

For on-premises and hybrid cloud-based deployments, create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

For cloud-based deployments, configure the client with the Cisco Webex Administration Tool. However, you can optionally set up a TFTP server to configure the client with settings that are not available in Cisco Webex Administration Tool.

For Cisco Jabber for iPhone and iPad and Cisco Jabber for Android, you must create a global configuration file to set up:

- Directory integration for on-premises deployments.
- Voicemail service credentials for hybrid-cloud deployments.

Note In most environments, Cisco Jabber for Windows and Cisco Jabber for Mac do not require any configuration to connect to services. Create a configuration file only if you require custom content such as automatic updates, problem reporting, or user policies and options.

Before you begin

Note the following configuration file requirements:

- Configuration filenames are case-sensitive. Use lowercase letters in the filename to prevent errors and to ensure the client can retrieve the file from the TFTP server.
- You must use utf-8 encoding for the configuration files.
- The client cannot read configuration files that do not have a valid XML structure. Check the structure of your configuration file for closing elements and confirm that elements are nested correctly.
- Valid XML character entity references only are permitted in your configuration file. For example, use `&` instead of `&`. If your XML contains invalid characters, the client cannot parse the configuration file.

  To validate your configuration file, open the file in Microsoft Internet Explorer.

  - If Internet Explorer displays the entire XML structure, your configuration file does is valid.
  - If Internet Explorer displays only part of the XML structure, it is likely that your configuration file contains invalid characters or entities.

Procedure

	Command or Action	Purpose
Step 1	Specify Your TFTP Server Address, on page 55	Specify your TFTP server address for client to enable access to your configuration file.
Step 2	Create Global Configurations, on page 56	Configure the clients for users in your deployment.
Step 3	Create Group Configurations, on page 56	Apply different configuration to different set of users.
Step 4	Host Configuration Files, on page 57	Host configuration files on any TFTP server.
Step 5	Restart Your TFTP Server, on page 58	Restart the TFTP server before the client can access the configuration files.

Specify Your TFTP Server Address

The client gets configuration files from a TFTP server. The first step in configuring the client is to specify your TFTP server address so the client can access your configuration file.

Attention If Cisco Jabber gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:

- Users manually enter the TFTP server address when they start the client.
- You specify the TFTP server address during installation with the TFTP argument.
- You specify the TFTP server address in the Microsoft Windows registry.

Create Global Configurations

The client downloads the global configuration file from your TFTP server during the login sequence. Configure the client for all users in your deployment.

Before you begin

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create a file named `jabber-config.xml` with any text editor.

- Use lowercase letters in the filename.
- Use UTF-8 encoding.

Step 2 Define the required configuration parameters in `jabber-config.xml`.

Step 3 Host the group configuration file on your TFTP server.

If your environment has multiple TFTP servers, ensure that the configuration file is the same on all TFTP servers.

Create Group Configurations

Group configuration files apply to subsets of users and are supported on Cisco Jabber for desktop (CSF devices) and on Cisco Jabber for mobile devices. Group configuration files take priority over global configuration files.

If you provision users with CSF devices, specify the group configuration filenames in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, set a unique configuration filename for each group during installation with the TFTP_FILE_NAME argument.

Before you begin

- If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create an XML group configuration file with any text editor.

The group configuration file can have any appropriate name; for example, `jabber-groupa-config.xml`.

Step 2 Define the required configuration parameters in the group configuration file.

Step 3 Add the group configuration file to applicable CSF devices.

a) Open the **Cisco Unified CM Administration** interface.
b) Select **Device** > **Phone**.
c) Find and select the appropriate CSF device to which the group configuration applies.
d) In the **Phone Configuration** window, navigate to **Product Specific Configuration Layout** > **Desktop Client Settings**.
e) In the **Cisco Support Field** field, enter `configurationfile=`*`group_configuration_file_name.xml`*. For example, enter `configurationfile=groupa-config.xml`.

Note If you host the group configuration file on your TFTP server in a location other than the default directory, you must specify the path and the filename; for example, `configurationfile=/customFolder/groupa-config.xml`.

Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.

f) Select **Save**.

Step 4 Host the group configuration file on your TFTP server.

Host Configuration Files

You can host configuration files on any TFTP server. However, Cisco recommends hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is the same as that where the device configuration file resides.

Procedure

Step 1 Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.

Step 2 Select **Software Upgrades** > **TFTP File Management**.

Step 3 Select **Upload File**.

Step 4 Select **Browse** in the **Upload File** section.

Step 5 Select the configuration file on the file system.

Step 6 Do not specify a value in the **Directory** text box in the **Upload File** section.

You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.

Step 7 Select **Upload File**.

Restart Your TFTP Server

You must restart your TFTP server before the client can access the configuration files.

Procedure

Step 1 Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.

Step 2 Select **Tools** > **Control Center - Feature Services**.

Step 3 Select **Cisco Tftp** from the **CM Services** section.

Step 4 Select **Restart**.

A window displays to prompt you to confirm the restart.

Step 5 Select **OK**.

The **Cisco Tftp Service Restart Operation was Successful** status displays.

Step 6 Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.

What to do next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL: `http://tftp_server_address:6970/jabber-config.xml`

Configuration File

For detailed information on the *jabber-config.xml* configuration file structure, group elements, parameters, and examples, see the Parameters Reference Guide for Cisco Jabber.

Set Parameters on Phone Configuration for Desktop Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

Enterprise Phone Configuration

Applies to the entire cluster.

Note For users with only IM and Presence Service capabilities (IM only), you must set phone configuration parameters in the **Enterprise Phone Configuration** window.

Common Phone Profile Configuration

Applies to groups of devices and takes priority over the cluster configuration.

Cisco Unified Client Services Framework (CSF) Phone Configuration

Applies to individual CSF devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Desktop Client Settings Configuration	Description
Video Calling	Enables or disables video capabilities. **Enabled (default)** Users can send and receive video calls. **Disabled** Users cannot send or receive video calls. **Restriction** This parameter is available only on the CSF device configuration.
File Types to Block in File Transfer	Restricts users from transferring specific file types. Set a file extension as the value, for example, `.exe`. Use a semicolon to delimit multiple values, for example, `.exe;.msi;.rar;.zip`
Automatically Start in Phone Control	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts. **Enabled** Use the desk phone device for calls. **Disabled (default)** Use the software phone (CSF) device for calls.
Jabber For Windows Software Update Server URL	Specifies the URL to the XML file that holds client update information. The client uses this URL to retrieve the XML file from your web server. In hybrid cloud-based deployments, you should use the Cisco WebexAdministration Tool to configure automatic updates.
Problem Report Server URL	Specifies the URL for the custom script that allows users to submit problem reports.

Set Parameters on Phone Configuration for Mobile Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

- Cisco Dual Mode for iPhone (TCT) Configuration — Applies to individual TCT devices and takes priority over the group configuration.
- Cisco Jabber for Tablet (TAB) Configuration — Applies to individual TAB devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Parameter	Description
On-Demand VPN URL	URL for initiating on-demand VPN. **Note** Applicable for iOS only.
Preset Wi-fi Networks	Enter the SSIDs for Wi-Fi networks (SSIDs) approved by your organization. Separate SSIDs with a forward slash (/). Devices do not connect to secure connect if connected to one of the entered Wi-Fi networks.
Default Ringtone	Sets the default ringtone to **Normal** or **Loud**.
Video Capabilities	Enables or disables video capabilities. • Enabled (default) — Users can send and receive video calls. • Disabled — Users cannot send or receive video calls.
Dial via Office **Note** TCT and BOT devices only.	Enables or disables Dial via Office. • Enabled — Users can dial via office. • Disabled (default) — Users cannot dial via office.

Configure Proxy Setting

The client uses proxy settings to connect to services.

The following limitations apply when using a proxy for these HTTP requests:

- Proxy Authentication is not supported.
- Wildcards in the bypass list are supported.
- Cisco Jabber supports proxy for HTTP request using HTTP CONNECT, but does not support proxy when using HTTPS CONNECT.

- Web Proxy Auto Discovery (WAPD) is not supported and must be disabled.

Configure Proxy Settings for Cisco Jabber for Windows

Configure proxy settings for Windows in the Local Area Network (LAN) settings for Internet properties.

Procedure

Step 1 In the **Connections** tab select **LAN Settings**.

Step 2 Configure a proxy using one of the following options:

- For automatic configuration, specify a `.pac` file URL.
- For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Mac

Configure proxy settings for Mac in **System Preferences**.

Procedure

Step 1 Select **System Preferences** > **Network**

Step 2 Choose your network service from the list and select **Advanced** > **Proxies** .

Step 3 Configure a proxy using one of the following options:

- For automatic configuration, specify a `.pac` file URL.
- For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber iPhone and iPad

Configure proxy settings in the Wi-Fi settings of an iOS device using one of the following methods:

Procedure

Step 1 Select **Wi-Fi** > **HTTP PROXY** > **Auto** and specify a `.pac` file URL as the automatic configuration script.

Step 2 Select **Wi-Fi** > **HTTP PROXY** > **Manual** and specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Android

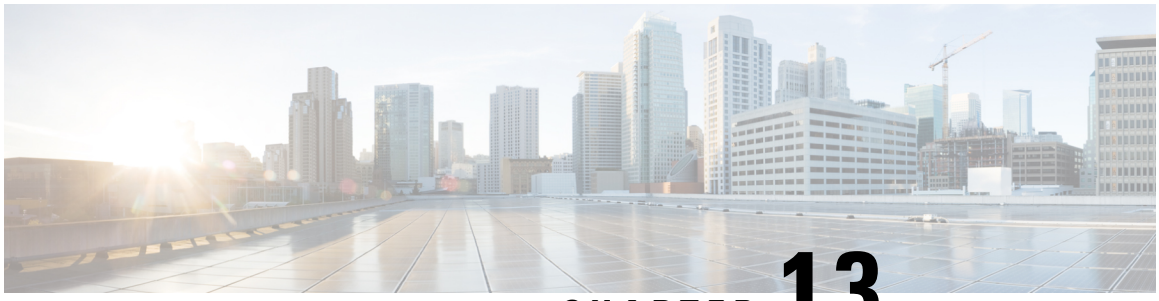
Procedure

Configure proxy settings in the Wi-Fi settings of an Android device using one of the following methods:

- Specify a .pac file URL as the automatic configuration script in the **Wi-Fi** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.

  Note This method is only supported on devices with Android OS 5.0 and later, and Cisco DX series devices.

- Specify an explicit proxy address in the **Wi-Fi Networks** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.



CHAPTER 13

Deploy Cisco Jabber Applications and Jabber Softphone for VDI

Download the Cisco Jabber Clients

If required, you can add your own Customer signature to the Jabber Installer or Cisco Dynamic Libraries by using the signing tools from the Operating System for that client.

Note For Cisco Jabber for Mac, the installer includes the product installer file. Use the Terminal tool to extract the pkg file from the installer and sign the pkg file before adding to the installer.

Procedure

- Visit the Cisco Software Center to download the Cisco Jabber for Mac and Cisco Jabber for Windows clients.
- For Cisco Jabber for Android, download the app from Google Play.
- For Cisco Jabber for iPhone and iPad, download the app from the App store.

Install Cisco Jabber for Windows

Cisco Jabber for Windows provides an MSI installation package that you can use in the following ways:

Install Option	Description
Use the Command Line, on page 64	You can specify arguments in a command line window to set installation properties. Choose this option if you plan to install multiple instances.
Run the MSI Manually, on page 81	Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client. Choose this option if you plan to install a single instance for testing or evaluation purposes.
Create a Custom Installer, on page 82	Open the default installation package, specify the required installation properties, and then save a custom installation package. Choose this option if you plan to distribute an installation package with the same installation properties.
Deploy with Group Policy, on page 86	Install the client on multiple computers in the same domain.

Before you begin

You must be logged in with local administrative rights.

Use the Command Line

Specify installation arguments in a command line window.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

```
msiexec.exe /i CiscoJabberSetup.msi
```

Step 3 Specify command line arguments as parameter=value pairs.

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

Step 4 Run the command to install Cisco Jabber for Windows.

Example Installation Commands

Review examples of commands to install Cisco Jabber for Windows.

Cisco Unified Communications Manager, Release 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
`/quiet` — Specifies a silent installation.

Related Topics

Command Line Arguments, on page 65
LCID for Languages, on page 80

Command Line Arguments

Review the command line arguments you can specify when you install Cisco Jabber for Windows.

Related Topics

Example Installation Commands, on page 64
LCID for Languages, on page 80

Override Argument

The following table describes the parameter you must specify to override any existing bootstrap files from previous installations:

Argument	Value	Description
CLEAR	1	Specifies if the client overrides any existing bootstrap file from previous installations. The client saves the arguments and values you set during installation to a bootstrap file. The client then loads settings from the bootstrap file at startup.

If you specify CLEAR, the following occurs during installation:

1. The client deletes any existing bootstrap file.
2. The client creates a new bootstrap file.

If you do not specify CLEAR, the client checks for existing bootstrap files during installation.

- If no bootstrap file exists, the client creates a bootstrap file during installation.
- If a bootstrap file exists, the client does not override that bootstrap file and preserves the existing settings.

Note If you are reinstalling Cisco Jabber for Windows, you should consider the following:

- The client does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate.
- The client does not save your installation arguments to an existing bootstrap file. If you want to change the values for installation arguments, or specify additional installation arguments, you must specify CLEAR to override the existing settings.

To override existing bootstrap files, specify CLEAR in the command line as follows:

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

Mode Type Argument

The following table describes the command line argument with which you specify the product mode:

Argument	Value	Description
PRODUCT_MODE	Phone_Mode	Specifies the product mode for the client. You can set the following value: • Phone_Mode — Cisco Unified Communications Manager is the authenticator. Choose this value to provision users with audio devices as base functionality.

When to Set the Product Mode

In phone mode deployments Cisco Unified Communications Manager is the authenticator. When the client gets the authenticator, it determines the product mode is phone mode. However, because the client always starts in the default product mode on the initial launch, users must restart the client to enter phone mode after sign in.

- Cisco Unified Communications Manager, Release 9.x and Later — You should not set PRODUCT_MODE during installation. The client gets the authenticator from the service profile. After the user signs in, the client requires a restart to enter phone mode.

Change Product Modes

To change the product mode, you must change the authenticator for the client. The client can then determine the product mode from the authenticator.

The method for changing from one product mode to another after installation, depends on your deployment.

Note In all deployments, the user can manually set the authenticator in the Advanced settings window.

In this case, you must instruct the user to change the authenticator in the Advanced settings window to change the product mode. You cannot override the manual settings, even if you uninstall and then reinstall the client.

Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later

To change product modes with Cisco Unified Communications Manager version 9.x and later, you change the authenticator in the service profile.

Procedure

Step 1 Change the authenticator in the service profiles for the appropriate users.

Change Default Mode > Phone Mode

Do not provision users with an IM and Presence service.

If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Change Phone Mode > Default Mode

Provision users with an IM and Presence service.

If you set the value of the **Product type** field in the IM and Presence profile to:

- **Unified CM (IM and Presence)** the authenticator is Cisco Unified Communications Manager IM and Presence Service.
- Webex **(IM and Presence)** the authenticator is the Cisco Webex Messenger service.

Step 2 Instruct users to sign out and then sign in again.

When users sign in to the client, it retrieves the changes in the service profile and signs the user in to the authenticator. The client then determines the product mode and prompts the user to restart the client.

After the user restarts the client, the product mode change is complete.

Authentication Arguments

The following table describe the command line arguments you can set to specify the source of authentication:

Argument	Value	Description
AUTHENTICATOR	CUP CUCM Webex	Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set one of the following as the value: • CUP—Cisco Unified Communications Manager IM and Presence Service. On-premises deployments in the default product mode. The default product mode can be either full UC or IM only. • CUCM—Cisco Unified Communications Manager. On-premises deployments in phone mode. • Webex—Cisco Webex Messenger Service. Cloud-based or hybrid cloud-based deployments. In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the `_cisco-uds` SRV record. The client can then automatically determine the authenticator.

Argument	Value	Description
CUP_ADDRESS	IP address Hostname FQDN	Specifies the address of Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) You should specify this argument if you set Cisco Unified Communications Manager as the authenticator. If you deploy: • In phone mode—you should specify the address of the TFTP server that hosts the client configuration. • In default mode—you can specify the address of the Cisco Unified Communications Manager TFTP service that hosts the device configuration.
CTI	IP address Hostname FQDN	Sets the address of your CTI server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • Users have desk phone devices and require a CTI server.

Argument	Value	Description
CCMCIP	IP address Hostname FQDN	Sets the address of your CCMCIP server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • The address of your CCMCIP server is not the same as the TFTP server address. The client can locate the CCMCIP server with the TFTP server address if both addresses are the same. Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.
SERVICES_DOMAIN	Domain	Sets the value of the domain where the DNS SRV records for Service Discovery reside. This argument can be set to a domain where no DNS SRV records reside if you want the client to use installer settings or manual configuration for this information. If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.
VOICE_SERVICES_DOMAIN	Domain	In Hybrid Deployments the domain required to discover Webex via CAS lookup may be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client will use the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection: • `_cisco-uds` • `_cuplogin` • `_collab-edge` This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration.

Argument	Value	Description
EXCLUDED_SERVICES	One or more of: • Webex • CUCM	Lists the services that you want Jabber to exclude from Service Discovery. For example, you may have done a trial with Webex which means that your company domain is registered on Webex, but you do not want Jabber users to authenticate using Webex. You want Jabber to authenticate with CUCM server. In this case set: • EXCLUDED_SERVICES=WEBEX Possible values are CUCM, Webex If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client.
UPN_DISCOVERY_ENABLED	true false	Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the User ID and domain for a user when discovering services. • true (default)—The UPN is used to find the User ID and the domain of the user, which is used during service discovery. Only the user discovered from UPN can log in to the client. • false—The UPN is not used to find the User ID and domain of the user. The user is prompted to enter credentials to find the domain for service discovery. Example installation command: `msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP Server Address

Cisco Jabber for Windows retrieves two different configuration files from the TFTP server:

- Client configuration files that you create.
- Device configuration files that reside on the Cisco Unified Communications Manager TFTP service when you provision users with devices.

To minimize effort, you should host your client configuration files on the Cisco Unified Communications Manager TFTP service. You then have only one TFTP server address for all configuration files and can specify that address as required.

You can, however, host your client configuration on a different TFTP server to the one that contains the device configuration. In this case, you have two different TFTP server addresses, one address for the TFTP server that hosts device configuration and another address for the TFTP server that hosts client configuration files.

Default Deployments

This section describes how you should handle two different TFTP server addresses in deployments that have a presence server.

You should do the following:

1. Specify the address of the TFTP server that hosts the client configuration on the presence server.
2. During installation, specify the address of the Cisco Unified Communications Manager TFTP service with the TFTP argument.

When the client starts for the first time, it:

1. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the bootstrap file.
2. Gets device configuration from the Cisco Unified Communications Manager TFTP service.
3. Connects to the presence server.
4. Retrieves the address of the TFTP service that hosts the client configuration from the presence server.
5. Gets client configuration from the TFTP server.

Phone Mode Deployments

This section describes how you should handle two different TFTP server addresses in phone mode deployments.

You should do the following:

1. During installation, specify the address of the TFTP server that hosts the client configuration with the TFTP argument.
2. Specify the address of the TFTP server that hosts the device configuration in your client configuration file with the following parameter: TftpServer1.
3. Host the client configuration file on the TFTP server.

When the client starts for the first time, it:

1. Retrieves the address of the TFTP server from the bootstrap file.
2. Gets client configuration from the TFTP server.
3. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the client configuration.
4. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

Common Installation Arguments

The following table describes command line arguments that are common to all deployments:

Argument	Value	Description
LANGUAGE	LCID in decimal	Defines the Locale ID (LCID), in decimal, of the language that Cisco Jabber for Windows uses. The value must be an LCID in decimal that corresponds to a supported language. For example, you can specify one of the following: • 1033 specifies English. • 1036 specifies French. See the *LCID for Languages* topic for a full list of the languages that you can specify. This argument is optional. If you do not specify a value, Cisco Jabber for Windows uses the regional language for the current user as the default. From Release 11.1(1) onwards, if you do not specify a value, Cisco Jabber for Windows checks the value for the UseSystemLanguage parameter. If the UseSystemLanguage parameter is set to true, the same language is used as for the operating system. If the UseSystemLanguage parameter is to set to false or not defined, then the client uses the regional language for the current user as the default. The regional language is set at **Control Panel** > **Region and Language** > **Change the date, time, or number format** > **Formats tab** > **Format dropdown**.
FORGOT_PASSWORD_URL	URL	Specifies the URL where users can reset lost or forgotten passwords. This argument is optional but recommended. **Note** In cloud-based deployments, you can specify a forgot password URL using the Cisco Webex Administration Tool. However, the client cannot retrieve that forgot password URL until users sign in.

Argument	Value	Description
AUTOMATIC_SIGN_IN	true false	Applies to Release 11.1(1) onwards. Specifies whether the **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • true—The **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • false (default)—The **Sign me in when Cisco Jabber starts** check box is not checked when the user installs the client.
TFTP_FILE_NAME	Filename	Specifies the unique name of a group configuration file. You can specify either an unqualified or fully qualified filename as the value. The filename you specify as the value for this argument takes priority over any other configuration file on your TFTP server. This argument is optional. **Remember** You can specify group configuration files in the **Cisco Support Field** on the CSF device configuration on Cisco Unified Communications Manager.

Argument	Value	Description
LOGIN_RESOURCE	WBX MUT	Controls user sign in to multiple client instances. By default, users can sign in to multiple instances of Cisco Jabber at the same time. Set one of the following values to change the default behavior: • WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the `wbxconnect` suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the `wbxconnect` suffix. • MUT—Users can sign in to one instance of Cisco Jabber for Windows at a time, but can sign in to other Cisco Jabber clients at the same time. Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix.
LOG_DIRECTORY	Absolute path on the local filesystem	Defines the directory where the client writes log files. Use quotation marks to escape space characters in the path, as in the following example: `"C:\my_directory\Log Directory"` The path you specify must not contain Windows invalid characters. The default value is `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`

Argument	Value	Description
CLICK2X	DISABLE Click2Call	Disables click-to-x functionality with Cisco Jabber. If you specify this argument during installation, the client does not register as a handler for click-to-x functionality with the operating system. This argument prevents the client from writing to the Microsoft Windows registry during installation. You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation. **Click2Call function in Browser**—The Click2X parameter can now be configured by using the newly added Click2Call parameter. This enables only the Click to call feature in the browser and disables the Click2X feature.
ENABLE_PRT	true false	• true (default)—The **Report a problem** menu item is enabled in the **Help** menu in the client. • false—The Jabber menu item option **Report a problem** is removed from the **Help** menu in the client. If you set the argument to false, users can still manually use the **Start Menu** > **Cisco Jabber** directory, or the Program files directory and launch the Problem Report Tool manually. If a user manually creates a PRT, and this parameter value is set to false, then the zip file created from the PRT has no content.
ENABLE_PRT_ENCRYPTION	true false	Enables problem report encryption. You must configure this argument with the PRT_CERTIFICATE_NAME argument. • true—PRT files sent by Jabber clients are encrypted. • false (default)—PRT files sent by Jabber clients are not encrypted. PRT encryption requires a public/private key pair to encrypt and decrypt the Cisco Jabber problem report.

Argument	Value	Description
PRT_CERTIFICATE_NAME	Certificate name	Specifies the name of a certificate with a public key in the Enterprise Trust or Trusted Root Certificate Authorities certificate store. The certificate public key is used to encrypt Jabber Problem reports. You must configure this argument with the ENABLE_PRT_ENCRYPTION argument.
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	Specifies the client behavior for invalid certificates. • RejectAndNotify—A warning dialog displays and the client doesn't load. • PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate. For invalid certificates in FIPS mode, this argument is ignored, the client displays a warning message and doesn't load.
Telemetry_Enabled	true false	Specifies whether analytics data is gathered. The default value is true. To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing. Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.

Argument	Value	Description
LOCATION_MODE	ENABLED DISABLED ENABLEDNOPROMPT	Specifies whether the Location feature is enabled and whether users are notified when new locations are detected. • ENABLED(default)—Location feature is turned on. Users are notified when new locations are detected. • DISABLED—Location feature is turned off. Users are not notified when new locations are detected. • ENABLEDNOPROMPT—Location feature is turned on. Users are not notified when new locations are detected.
FIPS_MODE	true false	Specifies whether Cisco Jabber is in FIPS mode. Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. Only connections with non-Windows APIs are in FIPS mode. If you don't include this setting, Cisco Jabber will determine the FIPS mode from the operating system.
SSO_EMAIL_PROMPT	ON OFF	Specifies whether the user is shown the email prompt for determining their home cluster. In order for the email prompt to work defined by ServicesDomainSsoEmailPrompt the installer requirements are: • SSO_EMAIL_PROMPT=ON • UPN_DISCOVERY_ENABLED=False • VOICE_SERVICES_DOMAIN=<domain_name> • SERVICES_DOMAIN=<domain_name> Example: msiexec.exe /i CiscoJabberSetup.msi SSO_EMAIL_PROMPT=ON UPN_DISCOVERY_ENABLED=False VOICE_SERVICES_DOMAIN=example.cisco.com SERVICES_DOMAIN=example.cisco.com CLEAR=1

Argument	Value	Description
ENABLE_DPI_AWARE	true false	Enables DPI awareness. DPI awareness enables Cisco Jabber to automatically adjust the display of text and images to suit different screen sizes. • true (default)— • on Windows 8.1 and Windows 10, Cisco Jabber adjusts to different DPI settings on each monitor. • on Windows 7 and Windows 8, Cisco Jabber displays according to the system DPI settings. • false—DPI awareness is not enabled. DPI awareness is enabled by default. To disable DPI awareness, use the following command: `msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false` **Note** If you are installing Cisco Jabber with the command line, remember to include the CLEAR=1 argument. If you are not installing Cisco Jabber from the command line, you must manually delete the jabber-bootstrap.properties file.

Argument	Value	Description
IP_Mode	IPv4-Only IPv6-Only Two Stacks	Specifies the network IP protocol for the Jabber client. • IPv4-Only—Jabber will only attempt to make IPv4 connections. • IPv6-Only—Jabber will only attempt to make IPv6 connections. • Two Stacks (Default)—Jabber can connect with either IPv4 or IPv6. **Note** IPv6-only support is available only for desktop devices on-premise deployment. All Jabber mobile devices must be configured as Two Stacks. For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release. There are a number of factors used to determine the network IP protocol used by Jabber, for more information see the IPv6 Requirements section in the *Planning Guide*.
DIAGNOSTICSTOOLENABLED	true false	Specifies whether the Cisco Jabber Diagnostics Tool is available to Cisco Jabber for Windows users. • true (default)—Users can display the Cisco Jabber Diagnostics Tool by entering Ctrl + Shift + D. • false—The Cisco Jabber Diagnostics Tool is not available to users.
FORWARD_VOICEMAIL	true false	Enables voicemail forwarding in the Voice Messages tab. • true (default)—Users can forward voicemails to contacts. • false—Voicemail forwarding is not enabled.

Argument	Value	Description
RESET_JABBER	1	Resets the user's local and roaming profile data. These folders are deleted: • `%appdata%\Cisco\Unified Communications\Jabber` • `%localappdata%\Cisco\Unified Communications\Jabber`

LCID for Languages

The following table lists the Locale Identifier (LCID) or Language Identifier (LangID) for the languages that the Cisco Jabber clients support.

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Arabic - Saudi Arabia	X		X	1025
Bulgarian - Bulgaria	X	X		1026
Catalan - Spain	X	X		1027
Chinese (Simplified) - China	X	X	X	2052
Chinese (Traditional) - Taiwan	X	X	X	1028
Croatian - Croatia	X	X		1050
Czech - Czech Republic	X	X		1029
Danish - Denmark	X	X	X	1030
Dutch - Netherlands	X	X	X	1043
English - United States	X	X	X	1033
Finnish - Finland	X	X		1035
French - France	X	X	X	1036
German - Germany	X	X	X	1031
Greek - Greece	X	X		1032

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Hebrew - Israel	X			1037
Hungarian - Hungary	X	X		1038
Italian - Italy	X	X	X	1040
Japanese - Japan	X	X	X	1041
Korean - Korea	X	X	X	1042
Norwegian - Norway	X	X		2068
Polish - Poland	X	X		1045
Portuguese - Brazil	X	X	X	1046
Portuguese - Portugal	X	X		2070
Romanian - Romania	X	X		1048
Russian - Russia	X	X	X	1049
Serbian	X	X		1050
Slovak - Slovakian	X	X		1051
Slovenian -Slovenia	X	X		1060
Spanish - Spain (Modern Sort)	X	X	X	3082
Swedish - Sweden	X	X	X	5149
Thai - Thailand	X	X		1054
Turkish	X	X		1055

Related Topics

Example Installation Commands, on page 64
Command Line Arguments, on page 65

Run the MSI Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the Advanced settings window.

Procedure

Step 1 Launch `CiscoJabberSetup.msi`.

The installation program opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.

Step 3 Start Cisco Jabber for Windows.

Step 4 Select **Manual setup and sign in**.

The Advanced settings window opens.

Step 5 Specify values for the connection settings properties.

Step 6 Select **Save**.

Create a Custom Installer

You can transform the default installation package to create a custom installer.

Note You use Microsoft Orca to create custom installers. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

Procedure

	Command or Action	Purpose
Step 1	Get the Default Transform File, on page 82	You must have the default transform file to modify the installation package with Microsoft Orca.
Step 2	Create Custom Transform Files, on page 83	Transform files contain installation properties that you apply to the installer.
Step 3	Transform the Installer, on page 83	Apply a transform file to customize the installer.

Get the Default Transform File

You must have the default transform file to modify the installation package with Microsoft Orca.

Procedure

Step 1 Download the Cisco Jabber administration package from Software Download page.

Step 2 Copy `CiscoJabberProperties.msi` from the Cisco Jabber administration package to your file system.

What to do next

Create Custom Transform Files, on page 83

Create Custom Transform Files

To create a custom installer, you use a transform file. Transform files contain installation properties that you apply to the installer.

The default transform file lets you specify values for properties when you transform the installer. You should use the default transform file if you are creating one custom installer.

You can optionally create custom transform files. You specify values for properties in a custom transform file and then apply it to the installer.

Create custom transform files if you require more than one custom installer with different property values. For example, create one transform file that sets the default language to French and another transform file that sets the default language to Spanish. You can then apply each transform file to the installation package separately. The result is that you create two installers, one for each language.

Before you begin

Get the Default Transform File, on page 82

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` and then apply `CiscoJabberProperties.msi`.

Step 3 Specify values for the appropriate installer properties.

Step 4 Generate and save the transform file.

a) Select **Transform** > **Generate Transform**.
b) Select a location on your file system to save the transform file.
c) Specify a name for the transform file and select **Save**.

The transform file you created is saved as *`file_name`*`.mst`. You can apply this transform file to modify the properties of `CiscoJabberSetup.msi`.

What to do next

Transform the Installer, on page 83

Transform the Installer

Apply a transform file to customize the installer.

Note Applying transform files will alter the digital signature of `CiscoJabberSetup.msi`. Attempts to modify or rename `CiscoJabberSetup.msi` will remove the signature entirely.

Before you begin

Create Custom Transform Files, on page 83

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` in Microsoft Orca.

a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

The installation package opens in Microsoft Orca. The list of tables for the installer opens in the **Tables** pane.

Step 3 Required: Remove all language codes except for 1033 (English).

Restriction You must remove all language codes from the custom installer except for 1033 (English).

Microsoft Orca does not retain any language files in custom installers except for the default, which is 1033. If you do not remove all language codes from the custom installer, you cannot run the installer on any operating system where the language is other than English.

a) Select **View** > **Summary Information**.

The **Edit Summary Information** window displays.

b) Locate the **Languages** field.
c) Delete all language codes except for 1033.
d) Select **OK**.

English is set as the language for your custom installer.

Step 4 Apply a transform file.

a) Select **Transform** > **Apply Transform**.
b) Browse to the location of the transform file on your file system.
c) Select the transform file and then select **Open**.

Step 5 Select **Property** from the list of tables in the **Tables** pane.

The list of properties for `CiscoJabberSetup.msi` opens in the right panel of the application window.

Step 6 Specify values for the properties you require.

Tip Values are case sensitive. Ensure the value you enter matches the value in this document.

Tip Set the value of the CLEAR property to `1` to override any existing bootstrap file from previous installations. If you do not override existing bootstrap files, the values you set in the custom installer do not take effect.

Step 7 Remove any properties that you do not require.

It is essential to remove any properties that are not being set, otherwise the properties being set will not take effect. Remove each property that is not needed one at a time.

a) Right-click the property you want to remove.
b) Select **Drop Row**.
c) Select **OK** when Microsoft Orca prompts you to continue.

Step 8 Required: Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 9 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

Installer Properties

The following are the properties you can modify in a custom installer:

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

These properties correspond to the installation arguments and have the same values.

Deploy with Group Policy

Install Cisco Jabber for Windows with Group Policy using the Microsoft Group Policy Management Console (GPMC) on Microsoft Windows Server.

Note To install Cisco Jabber for Windows with Group Policy, all computers or users to which you plan to deploy Cisco Jabber for Windows must be in the same domain.

Procedure

	Command or Action	Purpose
Step 1	Set a Language Code, on page 86	You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.
Step 2	Deploy the Client with Group Policy, on page 87	Deploy Cisco Jabber for Windows with Group Policy.

Set a Language Code

Altering the installation language is not necessary in Group Policy deployment scenarios where the exact MSI file provided by Cisco will be used. The installation language will be determined from the Windows User Locale (Format) in these situations. You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.

Procedure

Step 1 Start Microsoft Orca.

Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and ,NET Framework 4 that you can download from the Microsoft website.

Step 2 Open `CiscoJabberSetup.msi`.

a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

Step 3 Select **View** > **Summary Information**.

Step 4 Locate the **Languages** field.

Step 5 Set the **Languages** field to 1033.

Step 6 Select **OK**.

Step 7 Required: Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 8 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

What to do next

Deploy the Client with Group Policy, on page 87

Deploy the Client with Group Policy

Complete the steps in this task to deploy Cisco Jabber for Windows with Group Policy.

Before you begin

Set a Language Code, on page 86

Procedure

Step 1 Copy the installation package to a software distribution point for deployment.

All computers or users to which you plan to deploy Cisco Jabber for Windows must be able to access the installation package on the distribution point.

Step 2 Select **Start** > **Run** and then enter the following command:

```
GPMC.msc
```

The **Group Policy Management** console opens.

Step 3 Create a new group policy object.

a) Right-click on the appropriate domain in the left pane.
b) Select **Create a GPO in this Domain, and Link it here**.

The **New GPO** window opens.

c) Enter a name for the group policy object in the **Name** field.
d) Leave the default value or select an appropriate option from the **Source Starter GPO** drop-down list and then select **OK**.

The new group policy displays in the list of group policies for the domain.

Step 4 Set the scope of your deployment.

a) Select the group policy object under the domain in the left pane.

The group policy object displays in the right pane.

b) Select **Add** in the **Security Filtering** section of the **Scope** tab.

The **Select User, Computer, or Group** window opens.

c) Specify the computers and users to which you want to deploy Cisco Jabber for Windows.

Step 5 Specify the installation package.

a) Right-click the group policy object in the left pane and then select **Edit**.

The **Group Policy Management Editor** opens.

b) Select **Computer Configuration** and then select **Policies** > **Software Settings**.
c) Right-click **Software Installation** and then select **New** > **Package**.
d) Enter the location of the installation package next to **File Name**; for example, `\\server\software_distribution`.

Important You must enter a Uniform Naming Convention (UNC) path as the location of the installation package. If you do not enter a UNC path, Group Policy cannot deploy Cisco Jabber for Windows.

e) Select the installation package and then select **Open**.
f) In the **Deploy Software** dialog box, select **Assigned** and then **OK**.

Group Policy installs Cisco Jabber for Windows on each computer the next time each computer starts.

Configure Automatic Updates for Windows

To enable automatic updates, you create an XML file that contains the information for the most recent version, including the URL of the installation package on the HTTP server. The client retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.

Note If you use the Cisco Webex Messenger service for instant messaging and presence capabilities, you should use the Cisco Webex Administration Tool to configure automatic updates.

XML File Structure

XML files for automatic updates have the following structure:

```
<JabberUpdate>
          <App name="JabberWin">
               <LatestBuildNum>12345</LatestBuildNum>
               <LatestVersion>11.8.x</LatestVersion>
               <Mandatory>true</Mandatory>
               <Message>
                  <![CDATA[<b>This new version of Cisco Jabber lets you do the
                  following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
                  more information click <a target="_blank"
                  href="http://cisco.com/go/jabber">here</a>.]]>
               </Message>
               <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>

          </App>
        </JabberUpdate>
```

Before you begin

- Install and configure an HTTP server to host the XML file and installation package.
- Ensure users have permission to install software updates on their workstations.

Microsoft Windows stops update installations if users do not have administrative rights on their workstations. You must be logged in with administrative rights to complete installation.

Procedure

Step 1 Host the update installation program on your HTTP server.

Step 2 Create an update XML file with any text editor.

Step 3 Specify values in the XML as follows:

- `name`—Specify the following ID as the value of the `name` attribute for the `App` element:
  - JabberWin—The update applies to Cisco Jabber for Windows.
- `LatestBuildNum`—Build number of the update.
- `LatestVersion`—Version number of the update.
- `Mandatory`—(Windows clients only) True or False. Determines whether users must upgrade their client version when prompted.
- `Message`—HTML in the following format:

  `<![CDATA[your_html]]>`
- `DownloadURL`—URL of the installation package on your HTTP server.
- `AllowUpdatesViaExpressway`—(Windows client only). False (default) or True. Determines whether Jabber can carry out automatic updates while connected to the corporate network over the Expressway for Mobile and Remote Access.

  If your update XML file is hosted on a public web server, set this parameter to false. Otherwise the update file tells Jabber that it is hosted on an internal server that must be accessed through the Expressway for Mobile and Remote Access.

Step 4 Save and close your update XML file.

Step 5 Host your update XML file on your HTTP server.

Step 6 Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.

Uninstall Cisco Jabber for Windows

You can uninstall Cisco Jabber for Windows using either the command line or the Microsoft Windows control panel. This document describes how to uninstall Cisco Jabber for Windows using the command line.

Use the Installer

If the installer is available on the file system, use it to remove Cisco Jabber for Windows.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```

For example,

```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Use the Product Code

If the installer is not available on the file system, use the product code to remove Cisco Jabber for Windows.

Procedure

Step 1 Find the product code.

a) Open the Microsoft Windows registry editor.
b) Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`
c) Select **Edit** > **Find**.
d) Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.
e) Find the value of the **ProductIcon** key.

The product code is the value of the **ProductIcon** key, for example, `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.

Note The product code changes with each version of Cisco Jabber for Windows.

Step 2 Open a command line window.

Step 3 Enter the following command:

```
msiexec.exe /x product_code
```

For example,

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Install Cisco Jabber for Mac

Installer for Cisco Jabber for Mac

Installing the Client

You can choose to install the client using one of the following methods:

- Provide the installer for users to manually install the application. The client is installed in the `Applications` folder. Previous versions of the client need to be removed.
- Configure automatic updates for users, the installer silently updates the application.

  For automatic updates, the client is always added in the `Applications` folder.

  - If the client existed in a different folder, or a sub folder of the `Applications` folder, then a link is created in that folder to run the client in the Applications folder.
  - If the user previously renamed the client, then the installer will rename the new client to match.

Users are prompted for system credentials similar to installing other OS X installers.

Quiet Install—To install the client quietly, in the Terminal tool use the following Mac OS X command:

```
sudo installer -pkg /path_to/Install_Cisco-Jabber-Mac.pkg -target /
```

For more information on the installer command, refer to the installer manual pages on your Mac.

Accessories Manager

Accessories Manager is a component that provides Unified Communication control APIs to accessory device vendors. Third party devices can use these APIs to perform tasks such as mute audio, answer calls, and end calls from the device. Third party vendors write plugins that are loaded by the application. Standard headsets can be connected with speaker and microphone support. Only specific devices interact with Accessories Manager for call control. Please contact your devices vendor for more information. Desktop phones are not supported.

The client installer includes the third party plug-ins from the vendors. They are installed in the `/Library/Cisco/Jabber/Accessories/` folder.

Supported third party vendors:

- Logitech
- Sennheiser
- Jabra
- Plantronics

Accessories manager functionality is enabled by default and configured using the EnableAccessoriesManager parameter. You can disable specific Accessories Manager plugins from third party vendors using the BlockAccessoriesManager parameter.

Configuration

Provide configuration information for your users to sign into the client. Choose one of the following:

- Provide your users with a configuration URL with optional server information. For further information, see the *URL Configuration for Cisco Jabber for Mac* section.
- Provide your users with the server information to connect manually. For further information, see the *Manual Connection Settings* section.
- Service discovery—For more information, see the *Service Discovery* section.

Run Installer Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the **Preferences** settings.

Before you begin

Remove any older versions of the client.

Procedure

Step 1 Launch the `jabber-mac.pkg`.
The installer opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.
The installer prompts the user to enter the system credentials.

Step 3 Launch the client, using either a configuration URL or running the client directly.
Enter user credentials.

URL Configuration for Cisco Jabber for Mac

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
    - Webex—When you set this value, the client:

- Does not perform CAS lookup
- Looks for:
  - `_cisco-uds`
  - `_cuplogin`
  - `_collab-edge`

- CUCM—When you set this value, the client:
  - Does not look for `_cisco-uds`
  - Looks for:
    - `_cuplogin`
    - `_collab-edge`

- CUP—When you set this value, the client:
  - Does not look for `_cuplogin`
  - Looks for:
    - `_cisco-uds`
    - `_collab-edge`

You can specify multiple, comma-separated values to exclude multiple services.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF

- EnablePRTEncryption—Optional. Specifies that the PRT file is encrypted. Applies to Cisco Jabber for Mac.
  - true
  - false

- PRTCertificateName—Optional. Specifies the name of the certificate. Applies to Cisco Jabber for Mac.
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.

- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.

- True
- False

- DiagnosticsToolEnabled—Specifies whether the diagnostics tool is available in the client. The default is true.
  - True
  - False

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, you must use the following capitlization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `EnablePRTEncryption`
- `PRTCertificateName`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `IP_Mode`
- `DiagnosticsToolEnabled`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Configure Automatic Updates for Mac

To enable automatic updates, you create an XML file that contains the information for the most recent version, including the URL of the installation package on the HTTP server. The client retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.

Note If you use the Cisco Webex Messenger service for instant messaging and presence capabilities, you should use the Cisco Webex Administration Tool to configure automatic updates.

XML File Structure

The following is example XML file for automatic updates:

```
<JabberUpdate>
<App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>
</App>
</JabberUpdate>
```

Example XML File 2

The following is an example XML file for automatic updates for both Cisco Jabber for Windows and Cisco Jabber for Mac:

```
<JabberUpdate>
 <App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>

 </App>
 <App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2
  </li></ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
  </DownloadURL>
</App>
</JabberUpdate>
```

Before you begin

Install and configure an HTTP server to host the XML file and installation package.

Note Configure Web servers to escape special characters to ensure the DSA signature succeeds. For example, on Microsoft IIS the option is: **Allow double spacing**.

Procedure

Step 1 Host the update installation program on your HTTP server.

Step 2 Create an update XML file with any text editor.

Step 3 Specify values in the XML as follows:

- `name`—Specify the following ID as the value of the `name` attribute for the `App` element:
  - JabberWin—The update applies to Cisco Jabber for Windows.
  - JabberMac—The update applies to Cisco Jabber for Mac.
- `LatestBuildNum`—Build number of the update.
- `LatestVersion`—Version number of the update.
- `Mandatory`—True or False. Determines whether users must upgrade their client version when prompted.
- `Message`—HTML in the following format:

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL`—URL of the installation package on your HTTP server.

  For Cisco Jabber for Mac the URL file must be in the following format:

  ```
  Install_Cisco-Jabber-Mac-version-size-dsaSignature.zip
  ```

Step 4 Save and close your update XML file.

Step 5 Host your update XML file on your HTTP server.

Step 6 Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.

Install Cisco Jabber Mobile Clients

Procedure

Step 1 To install Cisco Jabber for Android, download the app from Google Play from your mobile device.

Step 2 To install Cisco Jabber for iPhone and iPad, download the app from the App Store from your mobile device.

URL Configuration for Cisco Jabber for Android, iPhone, and iPad

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
  - Webex—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM—When you set this value, the client:
    - Does not look for `_cisco-uds`
    - Looks for:
      - `_cuplogin`
      - `_collab-edge`
  - CUP—When you set this value, the client:
    - Does not look for `_cuplogin`
    - Looks for:
      - `_cisco-uds`
      - `_collab-edge`

  You can specify multiple, comma-separated values to exclude multiple services.

  If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.
- PRTCertificateUrl—Specifies the name of a certificate with a public key in the trusted root certificate store. Applies to Cisco Jabber mobile clients.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False
- ForceLaunchBrowser—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
  - True
  - False

Note ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, use the following capitalization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `PRTCertificateURL`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Mobile Configuration Using Enterprise Mobility Management

Before using Enterprise Mobility Management (EMM), ensure:

- The EMM vendor supports Android for Work or Apple Managed App Configuration.
- Android devices OS is 5.0 or later.

To allow users to launch Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, you can configure Cisco Jabber using Enterprise Mobility Management (EMM).

For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

If you want Jabber to run only on managed devices, then you can deploy certificate-based authentication, and enroll the client certificate through EMM.

You can configure Cisco Jabber for iPhone and iPad as the default dialer for the local contacts that are imported from Microsoft Exchange Server. Configure the profile with the **Exchange ActiveSync** and enter the value `com.cisco.jabberIM` in the **Default Audio Call App** field of the MDM configuration file.

When using EMM, disable URL configuration by setting the AllowUrlProvisioning parameter to False in the EMM application. For more information on configuring the parameter, refer to the topic *AllowUrlProvisioning Parameter*.

EMM vendors may allow different value types to be set in Application Configuration settings, but Cisco Jabber only reads String value types. In EMM, configure the following parameters:

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- FIPS_MODE
- AllowUrlProvisioning
- IP_Mode

FIPS_MODE Parameter

Use this parameter to enable or disable FIPS mode on Cisco Jabber mobile clients using EMM.

- *true*—Runs Cisco Jabber in FIPS mode.
- *false*—Does not run Cisco Jabber in FIPS mode.

  Example:`<FIPS_MODE>false</FIPS_MODE>`

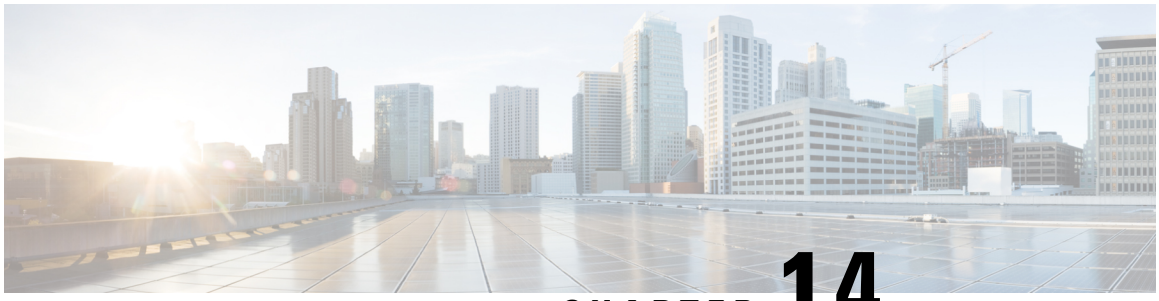
AllowUrlProvisioning Parameter

Use this parameter when migrating users from URL configuration to EMM.

The following values apply to this parameter:

- true (default)—Bootstrap configuration is performed using URL configuration
- false— Bootstrap configuration is not performed using URL configuration

  Example:`<AllowURLProvisioning>false</AllowURLProvisioning>`



CHAPTER 14

Remote Access

Service Discovery Requirements Workflow

Procedure

	Command or Action	Purpose
Step 1	Service Discovery Requirements, on page 49	
Step 2	DNS Requirements, on page 49	
Step 3	Certificate Requirements, on page 50	
Step 4	Test _collab-edge SRV Record, on page 102	

Service Discovery Requirements

Service discovery enables clients to automatically detect and locate services on your enterprise network. Expressway for Mobile and Remote Access allows you to access the services on your enterprise network. You should meet the following requirements to enable the clients to connect through Expressway for Mobile and Remote Access and discover services:

- DNS requirements
- Certificate requirements
- Test external SRV `_collab-edge`.

DNS Requirements

The DNS requirements for service discovery through remote access are:

- Configure a `_collab-edge` DNS SRV record on an external DNS server.
- Configure a `_cisco-uds` DNS SRV record on the internal name server.

- Optionally, for a hybrid cloud-based deployment with different domains for the IM and Presence server and the voice server, configure the Voice Services Domain to locate the DNS server with the `_collab-edge` record.

Note Jabber attempts connections to a maximum of three SSO-enabled servers, which are chosen randomly from all SSO-enabled servers that the DNS SRV records (`_collab-edge` and `_cisco-uds`) identify. If Jabber fails to connect three times, it considers Edge SSO unsupported.

Certificate Requirements

Before you configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.

For more information on configuring Cisco VCS Expressway certificate, see Configuring Certificates on Cisco VCS Expressway.

Test _collab-edge SRV Record

Test SRV Records

After creating your SRV records test to see if they are accessible.

Procedure

Step 1 Open a command prompt.

Step 2 Enter **nslookup**.
The default DNS server and address is displayed. Confirm that this is the expected DNS server.

Step 3 Enter **set type=SRV**.

Step 4 Enter the name for each of your SRV records.

For example `_cisco-uds.exampledomain`

- Displays server and address—SRV record is accessible.
- Displays `_cisco-uds.exampledomain: Non-existent domain`—There is an issue with your SRV record.

Cisco Anyconnect Deployment Workflow

Procedure

	Command or Action	Purpose
Step 1	Application Profiles, on page 103	
Step 2	Automate VPN Connection, on page 104	

	Command or Action	Purpose
Step 3	AnyConnect Documentation Reference, on page 107	
Step 4	Session Parameters, on page 107	

Cisco AnyConnect Deployment

Application Profiles

After you download the Cisco AnyConnect Secure Mobility Client to their device, the ASA must provision a configuration profile to the application.

The configuration profile for the Cisco AnyConnect Secure Mobility Client includes VPN policy information such as the company ASA VPN gateways, the connection protocol (IPSec or SSL), and on-demand policies.

You can provision application profiles for Cisco Jabber for iPhone and iPad in one of the following ways:

ASDM

We recommend that you use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client.

When you use this method, the VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA.

For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

iPCU

You can provision iOS devices using an Apple configuration profile that you create with the iPhone Configuration Utility (iPCU). Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use iPCU to create an Apple configuration profile.

   For more information, see the iPCU documentation.

2. Export the XML profile as a .mobileconfig file.

3. Email the .mobileconfig file to users.

   After a user opens the file, it installs the AnyConnect VPN profile and the other profile settings to the client application.

MDM

You can provision iOS devices using an Apple configuration profile that you create with third-party Mobile Device Management (MDM) software. Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use MDM to create the Apple configuration profiles.

   For information on using MDM, see the Apple documentation.

2. Push the Apple configuration profiles to the registered devices.

To provision application profiles for Cisco Jabber for Android, use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client. The VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA. For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Automate VPN Connection

When users open Cisco Jabber from outside the corporate Wi-Fi network, Cisco Jabber needs a VPN connection to access the Cisco UC application servers. You can set up the system to allow Cisco AnyConnect Secure Mobility Client to automatically establish a VPN connection in the background, which helps ensure a seamless user experience.

Note VPN will not be launched because Expressway for Mobile and Remote Access has the higher connection priority even if VPN is set to automatic connection.

Set Up Trusted Network Connection

The Trusted Network Detection feature enhances the user experience by automating the VPN connection based on the user's location. When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco Jabber automatically detects that it is outside the trusted network. After this occurs, Cisco AnyConnect Secure Mobility Client initiates the VPN to ensure connectivity to the UC infrastructure.

Note The Trusted Network Detection feature works with both certificate- and password-based authentication. However, certificate-based authentication provides the most seamless user experience.

Procedure

Step 1 Using ASDM, open the Cisco AnyConnect client profile.

Step 2 Enter the list of Trusted DNS Servers and Trusted DNS Domain Suffixes that an interface can receive when the client is within a corporate Wi-Fi network. The Cisco AnyConnect client compares the current interface DNS servers and domain suffix with the settings in this profile.

Note You must specify all your DNS servers to ensure that the Trusted Network Detection feature works properly. If you set up both the TrustedDNSDomains and TrustedDNSServers, sessions must match both settings to be defined as a trusted network.

For detailed steps for setting up Trusted Network Detection, see the *Trusted Network Detection* section in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Set Up Connect On-Demand VPN

The Apple iOS Connect On Demand feature enhances the user experience by automating the VPN connection based on the user's domain.

When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco AnyConnect automatically detects if it is connected to a domain that you specify in the AnyConnect client profile. If so, the application initiates the VPN to ensure connectivity to the UC infrastructure. All applications on the device including Cisco Jabber can take advantage of this feature.

Note Connect On Demand supports only certificate-authenticated connections.

The following options are available with this feature:

- **Always Connect** — Apple iOS always attempts to initiate a VPN connection for domains in this list.
- **Connect If Needed** — Apple iOS attempts to initiate a VPN connection to the domains in the list only if it cannot resolve the address using DNS.
- **Never Connect** — Apple iOS never attempts to initiate a VPN connection to domains in this list.

Attention Apple plans to remove the Always Connect option in the near future. After the Always Connect option is removed, users can select the Connect If Needed option. In some cases, Cisco Jabber users may have issues when using the Connect If Needed option. For example, if the hostname for the Cisco Unified Communications Manager is resolvable outside the corporate network, iOS will not trigger a VPN connection. The user can work around this issue by manually launching Cisco AnyConnect Secure Mobility Client before making a call.

Procedure

Step 1 Use the ASDM profile editor, iPCU, or MDM software to open the AnyConnect client profile.

Step 2 In the AnyConnect client profile, under the Connect if Needed section, enter your list of on-demand domains.

The domain list can include wild-card options (for example, cucm.cisco.com, cisco.com, and *.webex.com).

Set Up Automatic VPN Access on Cisco Unified Communications Manager

Before you begin

- The mobile device must be set up for on-demand access to VPN with certificate-based authentication. For assistance with setting up VPN access, contact the providers of your VPN client and head end.
- For requirements for Cisco AnyConnect Secure Mobility Client and Cisco Adaptive Security Appliance, see the *Software Requirements* topic.
- For information about setting up Cisco AnyConnect, see the *Cisco AnyConnect VPN Client Maintain and Operate Guides*.

Procedure

Step 1 Identify a URL that will cause the client to launch VPN on Demand.

a) Use one of the following methods to identify a URL that will cause the client to launch VPN on Demand.

- Connect if Needed
  - Configure Cisco Unified Communications Manager to be accessed through a domain name (not an IP address) and ensure that this domain name is not resolvable outside the firewall.
  - Include this domain in the "Connect If Needed" list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.
- Always Connect
  - Set the parameter in step 4 to a nonexistent domain. A nonexistent domain causes a DNS query to fail when the user is inside or outside the firewall.
  - Include this domain to the "Always Connect" list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.

    The URL must include only the domain name. Do not include a protocol or a path (for example, use "cm8ondemand.company.com" instead of "https://cm8ondemand.company.com/vpn".

b) Enter the URL in Cisco AnyConnect and verify that a DNS query on this domain fails.

Step 2 Open the **Cisco Unified CM Administration** interface.

Step 3 Navigate to the device page for the user.

Step 4 In the **Product Specific Configuration Layout** section, in the **On-Demand VPN URL** field, enter the URL that you identified and used in Cisco AnyConnect in Step 1.

The URL must be a domain name only, without a protocol or path.

Step 5 Select **Save**.

When Cisco Jabber opens, it initiates a DNS query to the URL (for example, ccm-sjc-111.cisco.com). If this URL matches the On-Demand domain list entry that you defined in this procedure (for example, cisco.com), Cisco Jabber indirectly initiates the AnyConnect VPN connection.

What to do next

- Test this feature.
  - Enter this URL into the Internet browser on the iOS device and verify that VPN launches automatically. You should see a VPN icon in the status bar.
  - Verify that the iOS device can connect to the corporate network using VPN. For example, access a web page on your corporate intranet. If the iOS device cannot connect, contact the provider of your VPN technology.
  - Verify with your IT department that your VPN does not restrict access to certain types of traffic (for example, if the administrator set the system to allow only email and calendar traffic).
- Verify that you set up the client to connect directly to the corporate network.

AnyConnect Documentation Reference

For detailed information on AnyConnect requirements and deployments review the documentation for your release at the following: https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

Session Parameters

You can configure ASA session parameters to improve performance for secure connections. For the best user experience, you should configure the following ASA session parameters:

- Datagram Transport Layer Security (DTLS) — DTLS is an SSL protocol that provides a data path that prevents latency and data loss.
- Auto Reconnect — Auto reconnect, or session persistence, lets Cisco AnyConnect Secure Mobility Client recover from session disruptions and re-establish sessions.
- Session Persistence — This parameter allows the VPN session to recover from service disruptions and re-establish the connection.
- Idle Timeout — Idle timeout defines a period of time after which ASA terminates secure connections, if no communication activity occurs.
- Dead-Peer Detection (DTD) — DTD ensures that ASA and Cisco AnyConnect Secure Mobility Client can quickly detect failed connections.

Set ASA Session Parameters

Cisco recommends that you set up the ASA session parameters as follows to optimize the end user experience for Cisco AnyConnect Secure Mobility Client.

Procedure

Step 1 Set up Cisco AnyConnect to use DTLS.

For more information, see the *Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections* topic in the *Configuring AnyConnect Features Using ASDM* chapter of the *Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*.

Step 2 Set up session persistence (auto-reconnect).

a) Use ASDM to open the VPN client profile.
b) Set the **Auto Reconnect Behavior** parameter to **Reconnect After Resume**.

For more information, see the *Configuring Auto Reconnect* topic in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* chapter (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Step 3 Set the idle timeout value.

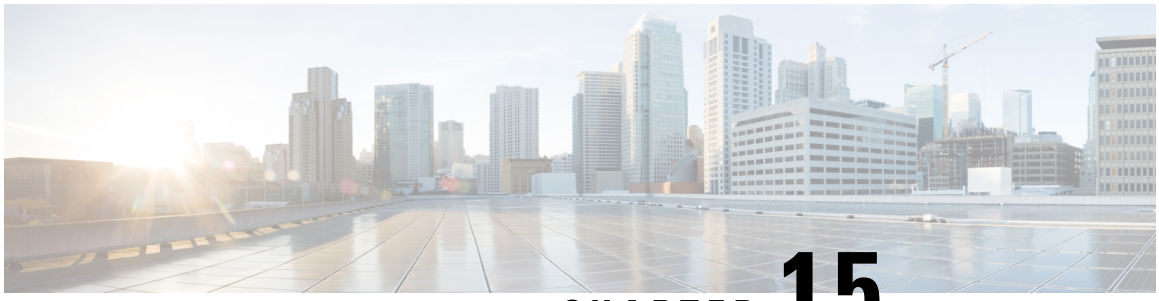
a) Create a group policy that is specific to Cisco Jabber clients.
b) Set the idle timeout value to 30 minutes.

For more information, see the *vpn-idle-timeout* section of the *Cisco ASA 5580 Adaptive Security Appliance Command Reference* for your release

Step 4 Set up Dead Peer Detection (DPD).

a) Disable server-side DPD.
b) Enable client-side DPD.

For more information, see the *Enabling and Adjusting Dead Peer Detection* topic of the *Configuring VPN* chapter of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*.



CHAPTER 15

Troubleshooting

Update the SSO Certificate for the Cisco Jabber Domain

This procedure applies to cloud or hybrid deployments. Use this procedure to upload an updated single sign-on (SSO) certificate for your Cisco Jabber domain.

Note Only certificates with 1024, 2048, or 4096 encryption bits and RC4-MD5 algorithms are supported.

Before you begin

The certificate must be in a .CER or .CRT file format.

Procedure

Step 1 Log in to the Webex Org Admin tool at https://www.webex.com/go/connectadmin.

Step 2 After loading the Administration tool, click the **Configuration** tab.

Step 3 In the left navigation bar, click on **Security Settings**.

Step 4 Click the link for **Organization Certificate Management**.
Previously imported X.509 certificates are displayed.

Step 5 In the **Alias** field, enter your company's Cisco Webex Organization.

Step 6 Click **Browse** to navigate to the X.509 certificate.
The certificate must be in a .CER or .CRT file format.

Step 7 Click **Import** to import the certificate.
If the certificate is not according to the format specified for an X.509 certificate, an error is displayed.

Step 8 Click **Close** twice to return to the **SSO Related Options** screen.

Step 9 Click **Save** to save your Federated Web single sign-on configuration details.

Cisco Jabber Diagnostics Tool

Windows and Mac

The Cisco Jabber Diagnostics Tool provides configuration and diagnostics information for the following functionality:

- Service Discovery
- Cisco Webex
- Cisco Unified Communications Manager Summary
- Cisco Unified Communications Manager Configuration
- Voicemail
- Certificate Validation
- Active Directory
- DNS Records

To access the Cisco Jabber Diagnostics Tool window, users must bring the hub window into focus and enter **`Ctrl + Shift + D`**. Users can update the data by clicking the **Reload** button. Users can also save the information to an html file by clicking the **Save** button.

The Cisco Jabber Diagnostics Tool is available by default. To disable this tool, you must set the DIAGNOSTICS_TOOL_ENABLED installation parameter to FALSE. For more information about this installation parameter, see *On-Premise Deployment for Cisco Jabber*, or *Cloud and Hybrid Deployments for Cisco Jabber*, depending on your setup.

Android, iPhone, and iPad

If users are unable to sign into Cisco Jabber or your Cisco Jabber IM and Phone services aren't connected, they can use the **Diagnose Error** option to check what's causing the issue.

Users can tap **Diagnose Error** option either from the **Sign In** page or from the warning notification they get when connecting to Cisco Jabber services. Cisco Jabber then verifies:

- If there are any network issues
- If Cisco Jabber servers are reachable
- If Cisco Jabber can reconnect

If any of these checks fail, Cisco Jabber displays an error report with the possible solution. If the issue persists, they can send a problem report.